

Sterling Integrator



Windows Cluster Environment Installation Guide

Version 5.1

Sterling Integrator



Windows Cluster Environment Installation Guide

Version 5.1

Note

Before using this information and the product it supports, read the information in "Notices" on page 81.

Copyright

This edition applies to Version 5 Release 1 of Sterling Integrator and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2000, 2012.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Chapter 1. Installation Overview 1

Installation Overview for a Windows Cluster	
Environment	1
Prerequisite Knowledge for Windows Installation	1
Intended Audience	1
Assumptions for this Guide	1

Chapter 2. Before You Begin the Installation 3

Before You Begin the Installation in a Windows Environment	3
System Verification Tasks for a Windows Environment	3
Preinstallation Checklist for a Windows Cluster Environment	3
Verify Your System Meets the System Requirements	5
Security Certificates	6
Multicast Ports: Node to Node Communications	6
Port Numbers in a Windows Environment	7
License File	7
Obtain a License File	8
Install the License Key (Windows)	8
Download the JCE Distribution File for the SUN JDK 1.6.	9

Chapter 3. Configure the Database. . . . 11

Supported Database Servers in a Windows Cluster Environment	11
Database Information You Need Before you Install Sterling Integrator in a Cluster Environment	11
Database Sizing and Capacity Planning	11
Database Definition Language (DDL) Statements	12
Configure DB2 with Sterling Integrator	12
DB2 Database Configuration Checklist	12
DB2 Parameters	13
Install DB2 Client Components, Compilers, and Fix Pack	13
Install JDBC Drivers for DB2	14
DB2 Database User Privileges	14
Configure Oracle with Sterling Integrator	14
Oracle Database Configuration Checklist	14
Configure an Oracle Instance	15
Configure Oracle Rollback	17
Install the Oracle JDBC Driver	17
Enable Failover in a Multiple Node Oracle RAC Database Cluster	17
Data Traffic Encryption in Oracle Database 11g Before You Encrypt Data Traffic for Oracle 11g Database	18
Configure Sterling Integrator for Data Traffic Encryption in Oracle (Windows)	19
Configure Sterling Integrator for Data Traffic Encryption in Oracle with SSL Authentication (Windows).	21

Configure Microsoft SQL Server with Sterling Integrator	24
Microsoft SQL Server Database Configuration Checklist	24
Microsoft SQL Server Database User Privileges	24
Install Microsoft SQL Server 2005 Service Pack and Hotfix.	25
Microsoft SQL Server Database Parameters	25
Install the JDBC Driver in Microsoft SQL Server 2005.	25
Configure Snapshot for Microsoft SQL Server	26
Database Password Management	26
Database Passwords	26
Database Passwords Encryption Methods	26
Encrypt Database Passwords (Windows).	26
Decrypt Database Passwords (Windows)	27

Chapter 4. Install the Software 29

General Installation/Upgrade Information for a Windows Cluster Environment	29
General Installation Wizard Information for Windows	29
Install Sterling Integrator (Windows Cluster)	30
Silent Installation	34
Create the Silent Installation File (Windows Cluster).	34
Install Sterling Integrator Using a Silent Installation File (Windows Cluster)	38
Configure the Sterling Integrator Desktop Icon for Windows Server 2008	40

Chapter 5. Validate the Installation. . . . 41

Validate the Installation Checklist in a Cluster Environment	41
Verify the Cluster Environment Settings in Property Files	41
Configure the Nodes in Windows Cluster	41
Access Sterling Integrator.	42
Validate the Installation	42
Stop a Node in the Windows Cluster Configuration (Hard Stop)	42
Stop Sterling Integrator (Windows Cluster).	43
Stop Sterling Integrator (Hardstop Windows)	43
Stop Cluster (Softstop Windows)	43
Restart the Windows Cluster	44

Chapter 6. Post Installation Configuration 45

Post Installation Configuration Checklist for Cluster Environment (Windows)	45
JMS Cluster Configuration for Failover	45
Configure ActiveMQ for a Cluster Environment (Windows).	46
Download Sterling Integrator Tools	47

Property Files Configuration in a Windows Environment	48
Configure Shared File Systems as Document Storage (Windows Cluster)	48
Add host[port] From all the Nodes to the jgroups_cluster.property.in for Each Node	49
Services and Adapters Associated with Node 1 in a Cluster	49
Configure Customer Overrides File with a Firewall between Nodes	50

Chapter 7. Installation Maintenance 51

Installation Maintenance for a Windows Cluster Environment	51
Determine If You Need to Apply a Maintenance Patch (Windows)	51
Preserve Custom Changes in Windows Cluster Environment	52
Install a Critical Maintenance Patch to the Cluster (Windows).	53
Install a Maintenance Patch One Node at Time to the Cluster (Windows).	54
Install a Hot-Fix (Windows Cluster)	56
Uninstalling an interim fix	57
DB Checksum Tool	57
Perform a Checksum (Windows)	57
Patch Changes Report	58
Example: Patch Changes Report	59

Chapter 8. Configure Non-English Environment in Windows 61

Non-English Environment Checklist	61
Language Settings in a Windows Environment	61
Install the Language Pack (Windows).	62
Load the Language Pack Translations (Windows).	62
Configure Encodings for the Sterling Integrator (Windows).	63
Configure Locales (Windows)	64
Load the Language Pack Factory Defaults (Windows).	64

Chapter 9. User Documentation 65

Sterling Integrator User Documentation	65
--	----

Access the Online Documentation	65
Request a Documentation CD	65

Chapter 10. Perimeter Server Installation 67

Perimeter Server Overview	67
Installation Guidelines for Perimeter Servers with Sterling Integrator	67
Perimeter Server Installation Methods	67
Perimeter Server Information Gathering Checklist	68
Perimeter Server Security Vulnerabilities.	68
Install a Perimeter Server in a Less Secure Network (Windows).	68
Install a Perimeter Server in a More Secure Network (Windows).	70
Silent Installation Method for an External Perimeter Server	71
Create the Silent Installation File for an External Perimeter Server.	71
Install an External Perimeter Server with a Silent Installation File (Windows)	72
Install Patches in a Remote Perimeter Server (Windows).	72
Grant Permissions for Specific Activities for a Perimeter Server.	73
Perform DNS Lookup on Remote Perimeter Server	74
Start Perimeter Servers (Windows).	75
Stop Perimeter Servers in (Windows).	75

Chapter 11. Uninstall the Software 77

Uninstall the Sterling Integrator from a Windows Cluster Environment	77
--	----

Chapter 12. Troubleshooting Tips for Windows 79

Troubleshooting Tips for Windows Environment	79
--	----

Notices 81

Chapter 1. Installation Overview

Installation Overview for a Windows Cluster Environment

Use this guide to install Sterling Integrator 5.1 in a Windows cluster environment.

This guide contains the following information:

- Before You Begin the Installation
- Configure the Database
- Install the Software
- Validate the Installation
- Post Installation Configuration
- Installation Maintenance
- Configure Non-English Environment
- User Documentation
- Perimeter Server Installation
- Uninstall the Software
- Troubleshooting Tips

Prerequisite Knowledge for Windows Installation

Before you begin the installation, you should be knowledgeable on the following topics:

- Application servers
- Database administration
- System Requirements for this release of Sterling Integrator

Intended Audience

This document is intended for use by:

- System Administrators
- Installation Engineers
- Database Administrators

Assumptions for this Guide

The procedures in this guide are accurate as of the publication date and are specific to Sterling Integrator 5.1.

Chapter 2. Before You Begin the Installation

Before You Begin the Installation in a Windows Environment

Before you begin the installation, you need to:

- Perform some system verification tasks
- Gather some information and complete the preinstallation worksheet

System Verification Tasks for a Windows Environment

Before you begin an installation, you need to:

#	System Verification Items	Your Notes
1	Use the system requirements to verify that your system hardware and software meet the requirements specified for this release. Verify you have the correct: <ul style="list-style-type: none">• Patches required by Java™ for the operation system• Version of the JDK• Absolute path to JDK and patches	
2	Verify the file system has adequate free disk space.	
3	Verify that your database has been installed and configured. If you are going to manually apply DDL statements, you need to complete the data base schema work before you begin the installation.	
4	If you are using a non-English environment, confirm that you are using the appropriate character set.	

Preinstallation Checklist for a Windows Cluster Environment

The preinstallation checklist contains the items you need to gather and tasks you need to complete prior to installing the Sterling Integrator. The checklist contains:

- Brief descriptions for tasks, while more detailed procedures are provided after the checklist
- Information you need to gather to complete the installation

You may want to make a copy of the following checklist and use it to record the information you collect for each node in the cluster.

The cluster environment does not support the following items:

- MySQL database
- AS2 Edition

#	Preinstallation Checklist	Node 1	Node 2	Your Notes
1	Determine which installation method you are going to use: <ul style="list-style-type: none"> • GUI • Silent Installation 			
2	Decide which type of security certificates you will use: <ul style="list-style-type: none"> • The default self-signed SSL (Secure Sockets Layer) certificate that is automatically installed. • A Certificate Authority-related certificate that you install before installing Sterling Integrator. 			
3	If you are using an Oracle, Microsoft SQL Server, or DB2 database, decide if you are going to manually or automatically apply Database Definition Language (DDL) Statements (schema) to the database.			
4	Determine if the database password need to be encrypted.			
5	Record the Hostname on which you plan to install Sterling Integrator.			
6	Record the Directory Name where you plan to install Sterling Integrator.			
7	Record the Login to host machine.			
8	Record the Password to the host machine.			
9	Record the path to the JDBC drivers.			
10	Record the path to the installation wizard and file name.			
11	Record the path to JDK.			
12	Record the path to the License File.			
13	Record the path to JCE file.			
14	Record the Host IP address.			
15	Record the Initial Port Number.			
16	Record the System passphrase.			

#	Preinstallation Checklist	Node 1	Node 2	Your Notes
17	Record the Database vendor name.			
18	Record the Database user name.			
19	Record the Database password.			
20	Record the Database (catalog) name.			
21	Record the Database host name.			
22	For Oracle and Microsoft SQL Server, record the Path and file name for the JDBC Driver.			
23	For DB2, record the Absolute paths and file names for two JDBC drivers.			
24	Obtain and install the license file.			
25	Determine if your windows environment is: <ul style="list-style-type: none"> • Windows 2003 or earlier • Windows Server 2008 			
26	Ensure you have read and write privileges on the parent installation directory.			

Verify Your System Meets the System Requirements

Before you begin the installation, verify that your system meets the hardware and software requirements specified for this release. The hardware requirements listed are the minimum required. Your system requirements will exceed these if you are running other applications on the same machine as the Sterling Integrator.

The installation strictly enforces the following *System Requirements*:

- Operating system version must match requirement exactly.
- The minimum patch level for the operating system is enforced, but you can apply higher patch levels.
- JDK version must match requirement exactly.
- The disk space is a minimum for the installation. The system should be separately sized to handle whatever load is going to be put on the system.
- Database version must match exactly.
- JDBC driver version supports exact matches and wildcard matches.

If any of the these requirements are not met, the installation will fail. If the installation fails, review the installation log for a list of non-compliant items.

Security Certificates

Before you begin the installation, you must decide which of the following security certificates you will use:

- The default self-signed SSL (Secure Sockets Layer) certificate that is automatically generated by the installation.
- A Certificate Authority-related certificate that you generate before installing the software.

If you install with the default SSL certificate, but you later want to switch to a CA-related certificate, you can make that change using the `sslCert` property in the `noapp.properties.in` file.

Multicast Ports: Node to Node Communications

Cluster nodes are configured to communicate with each other using JGroups, an open source toolkit that provides flexibility for protocol configuration. JGroups provides rich open management features, along with multiple protocol support. JGroups supports multicast (UDP) and TCP-based communication protocols.

When JGroups is configured to use multicast (UDP), all cluster nodes communicate with each other on a specific IP address and port. The multicast ports are configured based on the installation base port. All clusters that are on the same subnet configured on the same base port will send multicasting messages on the same multicast IP address and port.

To avoid this, each Sterling Integrator cluster on the same subnet needs to be configured on different base ports. Install your clusters on different port ranges or on different network segments with multicast forwarding restricted, so that they will not interfere with each other. The default multicast address used is 239.255.166.17. This address is configurable, with a port range of 10 ports, starting with the multicast base port for the instance.

All nodes participating in the same cluster must be installed on the same multicast base port (the `multicastBasePort` property in the `noapp.properties` file). This is usually computed from the system base (non-multicast) port, but can be configured separately in the `noapp.properties` file, to allow different nodes in a cluster to be installed at different (non-multicast) port ranges. Also, all the nodes in the cluster should be installed in the same subnet.

For node to node communications, the properties are defined in `jgroups_cluster.properties`. The attributes used to define communications are:

- `property_string` - default value is UDP.
- `distribution_property_string` - default value is TCP. This attribute should never be set to UDP.

If you want to change the communication for cluster multicast from the UDP protocol to TCP, you need to change the value of the `property_string` property in the `jgroups_cluster.properties.in` file (after backing up the file), and then run the `setupfiles.cmd` command. You can make this change right after the installation or after you have started running the cluster. If you change the file after starting the cluster, you need to stop all nodes of the cluster, make the change on each node, and then re-start your cluster.

To change the communication for cluster multicast from the UDP protocol to TCP, use the following value for the `property_string` property in the `jgroups_cluster.properties.in` file:

```
property_string=TCP(start_port=any_available_port_number):
TCPPING (initial_hosts=this_instance_host_ip[start_port_number],
theothernode_instance_host_ip[theothernode_start_port_number];port_range=2;
timeout=5000;num_initial_members=3;up_thread=true;down_thread=true):
VERIFY_SUSPECT(timeout=1500):
pbcast.NAKACK(down_thread=true;up_thread=true;gc_lag=100;retransmit_timeout=3000):
pbcast.GMS(join_timeout=5000;join_retry_timeout=2000;shun=false;print_local_addr=
true;down_thread=true;up_thread=true)
```

For more information about UDP, TCP, and JGroups communications, refer to the *Sterling Integrator Clustering* documentation.

Port Numbers in a Windows Environment

During installation or an upgrade, you are prompted to specify the initial port number for the Sterling Integrator.

To specify an initial port number, follow these guidelines:

- The Sterling Integrator requires a range of 200 consecutive open ports between 1025 and 65535. The port range starts with the initial port number and ends with the number that equals the initial port number plus 200. For example, if you specify 10100, then you need to make sure that 10100 through 10199 are not used by any other applications on your system
- The initial port number represents the beginning port number in the range.
- Make sure that port numbers in the port range are not used by any other applications on your system.

For the other ports after the initial port, you can accept the default port number suggested by the installation program, or you can individually re-assign pre-assigned default port numbers within the specified port range.

During the upgrade, about 50 default ports are pre-assigned for different services. For example, if you do not want xxx32 (10132) to be a default port, you could assign that port to xxx97 or another number within the port range.

After your installation or upgrade, refer to the `\install_dir\install\properties\sandbox.cfg` file for all of the port assignments.

License File

After your company signed the sales contract with Sterling Commerce, Sterling Commerce creates a license file containing information about your company, your system, and the packages (components) that your company selected to use, such as services, maps, and adapters.

Your first license file is a temporary keyfile that is e-mailed to you after you purchase Sterling Integrator. It allows you to run the software and all of the licensed features for a limited period. Before the keyfile expires, you must replace the temporary key with a permanent key. Failure to either extend your temporary keyfile or replace it with a permanent keyfile will result in the keyfile expiry and Sterling Integrator will fail to start.

The permanent license keyfile contains your specific operating system and the IP address of your system, and is valid for 20 years from the date of issue.

The permanent license file contains a single or multiple IP addresses in your computing environment. If you change an IP address in your computing environment that is present in your license file, the software will cease to operate. You should take necessary precautions to avoid this potential outage, including notifying the appropriate contacts within your organization (Information technology and related departments) and include the license file updates in your computing environment change plans.

Obtain a License File

About this task

To obtain a license file:

Procedure

1. Navigate to the Sterling Commerce Customer Center (<https://customer.sterlingcommerce.com>).
2. Click **Support Center > Sterling Integrator > Key Requests**.
3. Enter the following information:
 - Company Name
 - Contact Name
 - Phone Number
 - Fax number
 - Email Address
 - Requested Key Type (Permanent or Temporary)
 - PSP number - The PSP Number (unique number that identifies a licensed software asset in your Sterling Integrator installation) is present in the temporary or previous version of the keyfile you received from Sterling Commerce.
 - CD Key (if no PSP number is present in your license key)
 - Order Number
 - Product
 - Platform
 - Environment
 - IP Addresses
 - Previous IP Address
 - Sterling Account Executive
 - Comments
4. Click **Submit**.

Your new keyfile will be generated and delivered to you as an attachment to an email. Save this attachment and record the absolute path. This will be used during the install process.

Install the License Key (Windows)

About this task

To install the license key in a Windows environment:

Procedure

1. When you receive the permanent license keyfile, make a copy of it, and keep the copy in a safe place.
2. Stop Sterling Integrator.
3. Copy your license keyfile to the machine where Sterling Integrator is installed.
4. Navigate to `\install_dir\bin` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none">• Click Start.• Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

5. Enter `AddLicenseSet.cmd <path>`. Where `<path>` is the path to the license keyfile.
6. Start Sterling Integrator.
You can also install or update your license file from the Licenses screen (**Operations > System > Licenses**) when Sterling Integrator is running.

Download the JCE Distribution File for the SUN JDK 1.6

About this task

The Java Cryptography Extension (JCE) is a set of Java packages from Sun Microsystems, Inc. or IBM that provides a framework and implementations for encryption, key generation and key agreement, and Message Authentication Code (MAC) algorithms. By default, the software uses the limited strength JCE file that is included in the JDK that you use during the installation. Installing unlimited strength JCE file will overwrite the limited strength JCE file.

If you are installing the software outside of the United States, check to see if you can get the JCE unlimited strength jurisdiction policy files. The unlimited strength jurisdiction policy files can only be exported to countries to which the United States permits the export of higher-level encryption.

To obtain this file for the Sun JDK 1.6:

Procedure

1. Open your browser and navigate to <http://java.sun.com/javase/downloads/index.jsp>.
2. At the bottom of the page (Additional Resources), locate the **Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6** and click **Download**.
3. Click the [jce_policy-6.zip](#) link start the download.
4. Save the `jce_policy-6.zip` file to your system.
5. Record the directory and the zip file name. You will need this information during the installation process.

Chapter 3. Configure the Database

Supported Database Servers in a Windows Cluster Environment

In a windows cluster environment, the Sterling Integrator can support the following databases:

- Oracle®.
- DB2 .
- Microsoft SQL Server - In this document, where ever Microsoft SQL Server (MSSQL) is mentioned, it applies to both 2005 and 2008 depending on which version you have installed. If the information is specific to one version or the other version, the version is specifically stated.

Only a non-clustered installation can use the MySQL database. See *System Requirements* for supported version information.

You must install, create, and configure a database so that each Sterling Integrator instance has a dedicated schema and login for the database.

Database Information You Need Before you Install Sterling Integrator in a Cluster Environment

Before you begin to install Sterling Integrator, you need to install and configure your database. Review and gather the following information. An “x” indicates the information is required.

Information to Gather	Oracle	DB2	Microsoft SQL Server	Record Information Here
Database User Name	x	x	x	
Database Password	x	x	x	
Database Catalog Name	x	x	x	
Database Host	x	x	x	
Database Port	x	x	x	
JDBC Driver #1	x	x	x	
JDBC Driver #2		x		
Use BLOB data?	x		x	
Enable Multibyte Support?	x	x	x	

Database Sizing and Capacity Planning

Database sizing is designed to give you estimates of the database growth and to assist in planning the disk requirements.

There are many factors to consider when estimating the amount of disk space that will be required for the Sterling Integrator. As a result, trying to consider all growth factors is impractical because the user may not know the answers to many questions that are required to do a detailed forecast. Over the years the cost of

disks has dramatically decreased, and the capacity and speed of disks has increased. The method of how information system managers order disk capacity has also changed, from purchasing disk arrays that are dedicated to a particular database server and project, to the concept of SANS (Storage Area Network).

The Sterling Integrator provides a methodology to estimate your initial disk requirements. Consider the confidence that you have in your data estimates when making the final purchase decision and adjust accordingly. After the initial purchase and production deployment, disk growth should be tracked for future purchase forecasts.

You should track your actual database storage usage and the number of database records regularly. Correlating these two metrics enabled you to plan your future disk requirements. Moreover, determining the average amount of space used for each order line or shipment line, enables you to accurately predict your future growth requirements.

Database Definition Language (DDL) Statements

When you install Sterling Integrator, you can manually apply Database Definition Language (DDL) statements to your database tables instead of requiring the installation process to do it directly. This option is not available for MySQL databases.

This feature increases database security by reducing the database permissions of the Sterling Integrator database user. The rights to database objects can be reserved for a secure user like a customer database administrator (DBA). A business can require that only a DBA with the proper permissions can make database changes.

If you:	Then
Choose to manually apply the DDL statements	<p>Before you begin the installation, you will need to manually create the database schema using the sql files in the <code>\install_dir\install\repository\scripts</code> directory. For more information, refer to the utilities configuration documentation.</p> <p>You need to apply the DDL statements in a specific order. To find an example of the correct order, run an installation where the database schema was applied automatically and then look in the installation log file.</p> <p>The installation process will validate the database with a Sterling Integrator tool called DBVerify and warn you if there are issues, and will exit the installation.</p>
Choose NOT to manually apply the DDL statements	The installation will apply the DDL statements.

Configure DB2 with Sterling Integrator

DB2 Database Configuration Checklist

Before you begin:

- If you do not have the DB2 installed, follow the procedures in the DB2 Installation manual.

- The installation script creates tables and indexes. Certain tables require a page size of 32K. You should have a table space to accommodate such tables. DB2 automatically places tables and indexes in the available tablespaces using its internal logic. You can move the tables to a different tablespace after the installation is complete.
- If you are reinstalling the software, be aware that data in your existing database will be deleted. To prevent this, either back up the existing database or save it under a different name.
- After creating and configuring your database, recycle the database. Then stop and restart to apply the changes.

Use the following checklist to configure DB2 for Sterling Integrator:

#	DB2 Database Configuration Checklist	Your Notes
1	<p>Create the database.</p> <p>Refer to the DB2 documentation on creating the database, including creating a schema repository, login, and tablespace.</p> <p>Be sure to install the correct version and patches. See System Requirements for supported version information.</p>	
2	Install Client Components, Compilers, and Fix Pack.	
3	Review the DB2 Parameters.	
4	Ensure the DB2 User Privileges are set.	
5	Install JDBC Drivers for DB2.	

DB2 Parameters

The following parameters settings are required for your DB2 database:

Parameter	Value
DB2_SKIPDELETED	ON
DB2_SKIPINSERTED	ON
DB2_NUM_CKPW_DAEMONS	0
DB2LOCK_TO_RB	STATEMENT
LOCKLIST	AUTOMATIC
MAXLOCKS	AUTOMATIC If AUTOMATIC is not support, then 100
Database code page	UTF-8

For additional information, see the Performance Management documentation.

Install DB2 Client Components, Compilers, and Fix Pack

About this task

The Sterling Integrator uses stored procedures for DB2. You must install or set up the following components:

Procedure

1. Install the Administration client.
2. Install the necessary fix pack after you install the client components and compilers. Otherwise, the clients will overwrite the fix pack binaries.
3. Set the path for the compiler by using the **db2set** command.

What to do next

For more information about these tasks, see the IBM documentation.

Install JDBC Drivers for DB2

About this task

For DB2, install the appropriate DB2 JDBC Type 4 driver and any correlating patches. See *System Requirements* for supported version information.

You can obtain these files from the IBM Web site. After you obtain this JDBC driver, record the absolute path to its location on your system. You must supply this absolute path during installation.

If the JDBC driver provided by your database vendor is distributed among multiple files, you must place all the files that comprise the JDBC driver into one .jar file. Follow these steps to create one .jar file:

Procedure

1. Identify all the vendor database jar files for the JDBC driver.
2. Create a temporary working directory (`mkdir wd; cd wd`).
3. Extract the contents of each file used for the JDBC driver using the jar utility into the temporary working directory (`jar xvf <jdbc.jar>` for each supplied jar file). Various Sterling Integrator scripts, such as the one used for loading the factory defaults, specify a `DB_DRIVER`. The `DB_DRIVER` specified must include all of these JAR files. The `DB_DRIVER` setting is located in `sandbox.cfg`.
4. Bundle the files in the temporary working directory into one file using the jar utility (`jar cvf new.jar*`).
5. Record the absolute path to the .jar file you created on the Preinstallation Checklist.

The type-4 driver does not require a separate Java listener running on the database server. Instead, connect directly to the DB2 port.

DB2 Database User Privileges

The DBADM role is required for performing administrative operations in DB2 database.

Configure Oracle with Sterling Integrator

Oracle Database Configuration Checklist

About this task

You can use an Oracle database for maintaining information on Sterling Integrator.

Before you begin:

- If you are reinstalling the software, be aware that data in your existing database will be deleted. To prevent this, either back up the existing database or save it under a different name.
- After creating and configuring your database, recycle the database. Then stop and restart to apply the changes.

Use the following checklist to configure Oracle for Sterling Integrator:

#	Oracle Database Configuration Checklist	Your Notes
1	<p>Create the database.</p> <p>Refer to the Oracle documentation on creating the database, including creating a schema repository, login, and tablespace.</p> <p>Be sure to install the correct version and patches.</p> <p>See <i>System Requirements</i> for supported version information.</p>	
2	Configure an Oracle Instance.	
3	Configure Oracle Rollback.	
4	Install the Oracle JDBC Driver.	
5	Enable Failover in a Multiple Node Oracle RAC Database Cluster.	
6	<p>After Sterling Integrator is installed, if you want to encrypt the data traffic, perform one of the following tasks:</p> <ul style="list-style-type: none"> • Configure Sterling Integrator for Data Traffic Encryption • Configure Sterling Integrator for Data Traffic Encryption with SSL 	

Configure an Oracle Instance

About this task

Before you begin:

- You must have the Oracle database installed. Ensure you have installed the correct versions and patches. See *System Requirements* for supported version information.
- Ensure that the user responsible for creating and modifying the Oracle database has a specified quota (extent) assigned in the tablespace, even if the user was assigned an unlimited tablespace. Otherwise, the installer may throw the error *ORA-09150: no privileges on tablespace name*.

To configure the Oracle database:

Procedure

1. Run the create instance procedure. Use AL32UTF8 as the character set.
2. Configure the INIT<INSTANCE_NAME>.ORA file. The following parameter settings are required:

Parameter	Parameter Definition	Value
OPEN_CURSORS	Number of open cursors	Greater than or equal to 2000
SHARED_POOL_SIZE	Shared pool size	Greater than or equal to 90000000
LARGE_POOL_SIZE	Large pool size	Greater than or equal to 614400
JAVA_POOL_SIZE	Java pool size	Greater than or equal to 20971520
PROCESSES	Number of processes	Greater than or equal to 500 Must be greater than the number of connections required by Sterling Integrator (sum of transactional or local and NoTrans pools in jdbc.properties), and operational management tools.
LOG_BUFFER	Log buffer	Greater than or equal to 163840
DB_BLOCK_SIZE	Database block size	Greater than or equal to 8192
NLS_LENGTH_SEMANTICS	NLS Length semantics	CHAR When you change the multi-byte character set to CHAR, Oracle reserves space equivalent to "n" characters, which is more than "n" bytes.
SGA_MAX_SIZE	SGA maximum size	1 GB to <i>n</i> GB, depending on the amount of physical memory on your database server. If the server is running only this database, up to 80% of physical memory.
SGA_TARGET	SGA components total size	1 GB to <i>n</i> GB, depending on the amount of physical memory on your database server. If the server is running only this database, up to 80% of physical memory.
PGA_AGGREGATE_TARGET	PGA target aggregate memory	1 GB to <i>n</i> GB, depending on the amount of physical memory on your database server. If the server is running only this database, up to 80% of physical memory.
cursor_sharing	Cursor sharing	exact
timed_statistics	Timed Statistics	true
optimizer_mode	Optimizer mode	All_rows
db_cache_size	Database cache size	Greater than or equal to 19200

3. Identify or create a tablespace for user tables and indexes.
4. Create a user. Unless specifically stated for a given task, the user does not require database administrator (DBA) privileges.
5. Grant permissions to the user. The following permissions are required for the administrative user for creating and modifying the Oracle database: GRANT "CONNECT" TO SI_USER ALTER USER SI_USER DEFAULT ROLE "CONNECT" GRANT CREATE SEQUENCE TO SI_USER GRANT CREATE TABLE TO SI_USER GRANT CREATE TRIGGER TO SI_USER GRANT SELECT ON CTXSYS.CTX_USER_INDEXES TO SI_USER GRANT SELECT ON SYS.DBA_DATA_FILES TO SI_USER GRANT SELECT ON

```

SYS.DBA_FREE_SPACE TO SI_USER GRANT SELECT ON SYS.DBA_USERS
TO SI_USER GRANT SELECT ON SYS.V_$PARAMETER TO SI_USER GRANT
SELECT ANY DICTIONARY TO SI_USER GRANT ALTER SESSION TO
SI_USER GRANT CREATE SESSION TO SI_USER

```

6. If you are using Oracle AQ, grant the AQ_ADMINISTRATOR_ROLE permission.

Configure Oracle Rollback

About this task

You can rollback changes in Oracle using AUTO UNDO management. It is recommended that you use this option. This will avoid any manual monitoring of UNDO segments.

If a server is upgraded from Oracle 8i, set the UNDO_MANAGEMENT=AUTO parameter in init< SID>.ora. Your database administrator needs to determine the UNDO_RETENTION setting. Ensure that the file system, which has the UNDOTBS1 tablespace, has enough space to use the AUTOGROW setting.

Install the Oracle JDBC Driver

The Sterling Integrator requires the appropriate JDBC driver for Oracle Database. These drivers are thin client based pure Java JDBC drivers. See *System Requirements* for supported version information. The supported versions of the JDBC driver will build the correct Sterling Integrator directory structure.

Enable Failover in a Multiple Node Oracle RAC Database Cluster

About this task

To enable failover in a multiple node Oracle RAC database cluster in Windows:

Procedure

1. Navigate to `\install_dir\install\properties` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. <p>The Administrator: Command Prompt dialog box is displayed.</p>

2. In the `sandbox.cfg` file, add a new property for `ORACLE_JDBC_URL`, which contains the Oracle RAC connection URL.

The following example shows the suggested URL form and the way it is organized to connect using Service Name or System ID (SID). You can use either one of these identifiers when adding a URL, however, be aware that Oracle plans to deprecate use of SID.

The property value must be one string of text starting with `ORACLE_JDBC_URL=`. Your database administrator (DBA) can modify this URL as needed.

```

jdbc:oracle:thin:@
  (DESCRIPTION=
    (ADDRESS_LIST=
      (FAILOVER=ON)
      (LOAD_BALANCE=OFF)
      (ADDRESS=(PROTOCOL=TCP) (HOST=myhost1) (PORT=1521))
      (ADDRESS=(PROTOCOL=TCP) (HOST=myhost2) (PORT=1521))
    )
    (CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = myservicename OR mySID))
  )

```

3. Navigate to `\install_dir\install\bin` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

4. Enter `setupfiles.cmd`.

Data Traffic Encryption in Oracle Database 11g

You can encrypt transactions between Sterling Integrator and Oracle Database 11g. This prevents anyone outside the system from viewing the data while it tracks between the Sterling Integrator and the database.

The following is a list of important aspects of enabling database encryption with Sterling Integrator:

- The default configuration for encryption at installation is no encryption. If you want to have your database transactions to be encrypted, you must perform the tasks provided in this topic.
- The encryption can be enabled at any time.
- Once you enable encryption, it applies to all database transactions between Sterling Integrator and the database.

System performance may be impacted when encryption is enabled. The extent of this impact will depend on your hardware, database configuration, transaction volume, and the relative amount of processing time spent by the system against other activities.

Addition information on data traffic configuration can be found in the Oracle® documentation, which can be accessed from http://www.oracle.com/technology/tech/java/sqlj_jdbc/pdf/wp-oracle-jdbc_thin_ssl.pdf.

Before You Encrypt Data Traffic for Oracle 11g Database

Consider the following when configuring database traffic encryption:

- Sterling Integrator must be installed in TCP (clear) mode before you can configure encryption.
- You should perform these changes to your database prior to installing Sterling Integrator.
- You should configure wallets for encryption only mode even if the wallet used is empty. Enable auto login for all wallets.

- If you want to use SSL for encryption only, it is recommended to follow the instructions in the Oracle *CASE #1: USE SSL FOR ENCRYPTION ONLY* section of the Oracle documentation. It is not necessary to configure certificates for the wallet. In this mode, Diffie-Hellman ciphers are used and neither the server nor the client is authenticated through SSL. You must authenticate by using a username and a password. However, if you are running Sterling Integrator on a platform that requires an IBM JDK, you cannot use this mode, as IBM JSSE TrustManager does not permit anonymous ciphers. You must configure wallets with certificates.
- If you want to use SSL for encryption and for server authentication, it is recommended to follow the instructions in the Oracle *CASE #2: USE SSL FOR ENCRYPTION AND SERVER AUTHENTICATION* section of the Oracle documentation.
- If you want to use SSL for encryption and for server authentication of both tiers, it is recommended to follow the instructions in the Oracle *CASE #3: USE SSL FOR ENCRYPTION AND AUTHENTICATION OF BOTH TIERS* section of the Oracle documentation, depending on how you intend to configure client and/or server authentication.
- Once you configure your database for data traffic encryption, the database accepts both TCP (clear) and TCPS (encrypted) connections.
- There is a known issue in Oracle Database 11g when the listener is configured only for TCPS. The `lsnrctl` utility (that is used to start/stop DB listeners) attempts to contact the listener, which is enabled first. You should define the address list of the listener to contact either TCP or IPC before contacting TCPS.

Configure Sterling Integrator for Data Traffic Encryption in Oracle (Windows)

About this task

Use this procedure if you want to enable encryption only, with anonymous authentication, and not SSL authentication.

If you want to use SSL for encryption only, it is recommended to follow the instructions in the Oracle *CASE #1: USE SSL FOR ENCRYPTION ONLY* section of the Oracle documentation. It is not necessary to configure certificates for the wallet. In this mode, Diffie-Hellman ciphers are used and neither the server nor the client is authenticated through SSL. You must authenticate by using a username and a password. However, if you are running Sterling Integrator on a platform that requires an IBM JDK, you cannot use this mode, as IBM JSSE TrustManager does not permit anonymous ciphers. You must configure wallets with certificates.

This procedure is applicable only if you are running Sterling Integrator on a platform that requires Sun JDK. The IBM JSSE TrustManager does not permit anonymous ciphers.

If your Sterling Integrator is a cluster installation, you will need to perform this procedure on each node, starting with node 1.

Procedure

1. Install Sterling Integrator in TCP (clear) mode.
2. Stop Sterling Integrator.
3. Navigate to `\install_dir\install\properties` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

4. Open the customer_overrides.properties file and add the following additional database connection information:

```
jdbcService.oraclePool.prop_oracle.net.ssl_cipher_suites= (
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA, SSL_DH_anon_WITH_RC4_128_MD5,
SSL_DH_anon_WITH_DES_CBC_SHA)
jdbcService.oraclePool.prop_oracle.net.ssl_server_dn_match=false
```

If you have a container configured, ensure that the same database information is added to the customer_overrides.properties.in file. To locate the file, navigate to `\install_dir\install\properties\nodexACy`. Where *x* gives the node number and *y* gives the container number. Perform this step for all the containers configured in the system.

5. Repeat Step 4 for the following Oracle connection pools by changing only the poolname:

- oraclePool_local
- oraclePool_NoTrans
- oracleArchivePool
- oracleUIPool

If you have any other database pools, you will need to add the properties for those pools.

6. Open the sandbox.cfg file and change the database connection information as shown:

```
ORACLE_JDBC_URL= jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)
(HOST=<DB host>)(PORT=<TCPS port as configured in DB config section above>))
(CONNECT_DATA=(SERVICE_NAME=<service name>)))
```

Make sure you enter the HOST, PORT, and SERVICE_NAME.

7. Open the activemqconfig.xml.in file and modify the database connection information:

- Remove or comment out the following default ActiveMQ database configuration information:

```
<bean id="gis-ds" class="org.apache.commons.dbcp.BasicDataSource"
destroy-method="close" singleton="true" lazy-init="default"
autowire="default" dependency-check="default"
SCIOVERRIDEName="persistence-bean">
<property name="driverClassName">
<value>oracle.jdbc.driver.OracleDriver</value>
</property>
<property name="url">
#:ifdef ORACLE_JDBC_URL
<value>&ORACLE_JDBC_URL;</value>
#:else
<value>jdbc:oracle:thin:@&ORA_HOST;:&ORA_PORT;:&ORA_DATA;</value>
#:endif
</property>
<property name="username">
<value>&ORA_USER;</value>
```

```

</property>
<property name="password">
<value>&ORA_PASS;</value>
</property>
<property name="maxActive">
<value>32</value>
</property>
</bean>

```

- Add the following ActiveMQ database configuration information:

```

<bean id="gis-ds"
class="oracle.jdbc.pool.OracleDataSource" destroy-method="close"
singleton="true" lazy-init="default"
autowire="default"
dependency-check="default">
<property name="URL"><value>&ORACLE_JDBC_URL;</value></property>
<property name="user"><value>&ORA_USER;</value></property>
<property name="password"><value>&ORA_PASS;</value></property>
<property name="connectionProperties"><value> oracle.net.ssl_cipher_suites:
(SSL_DH_anon_WITH_3DES_EDE_CBC_SHA, SSL_DH_anon_WITH_RC4_128_MD5,
SSL_DH_anon_WITH_DES_CBC_SHA)
oracle.net.ssl_client_authentication: false
oracle.net.ssl_version: 3.0
driverClassName:oracle.jdbc.driver.OracleDriver
maxActive: 32
</value>
</property>
</bean>

```

8. Navigate to `\install_dir\install\bin` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

9. Enter `StartWindowsService.cmd`.
10. Restart Sterling Integrator. All the database connections from Sterling Integrator are now connected through TCPS (encrypted) mode.

Configure Sterling Integrator for Data Traffic Encryption in Oracle with SSL Authentication (Windows)

About this task

Use this procedure to enable encryption and SSL authentication. This procedure is applicable if you are running Sterling Integrator on a platform that requires either Sun JDK or IBM JDK.

The example in this procedure uses 2-way SSL authentication. If you want to use SSL for encryption and for server authentication, it is recommended to follow the instructions in the Oracle *CASE #2: USE SSL FOR ENCRYPTION AND SERVER AUTHENTICATION* section of the Oracle documentation.

You can also configure 1-way SSL authentication. If you want to use SSL for encryption and for server authentication of both tiers, it is recommended to follow the instructions in the Oracle *CASE #3: USE SSL FOR ENCRYPTION AND AUTHENTICATION OF BOTH TIERS* section of the Oracle documentation,

depending on how you intend to configure client and/or server authentication. For more information about 1-way SSL authentication, refer to Oracle® documentation, which can be accessed from http://www.oracle.com/technology/tech/java/sqlj_jdbc/pdf/wp-oracle-jdbc_thin_ssl.pdf.

If your Sterling Integrator is a cluster installation, you will need to perform this procedure on each node, starting with node 1.

Procedure

1. Install Sterling Integrator in TCP (clear) mode.
2. Stop Sterling Integrator.
3. Navigate to `\install_dir\install\properties` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. <p>The Administrator: Command Prompt dialog box is displayed.</p>

4. Open the `customer_overrides.properties` file and add additional database connection information:

```
jdbcService.oraclePool.prop_javax.net.ssl.trustStore=../../path/.../ClientKeyStore.jks
jdbcService.oraclePool.prop_javax.net.ssl.trustStoreType=JKS
jdbcService.oraclePool.prop_javax.net.ssl.trustStorePassword=password
jdbcService.oraclePool.prop_oracle.net.ssl_version=3.0
jdbcService.oraclePool.prop_javax.net.ssl.keyStore=../../path/.../ClientKeyStore.jks
jdbcService.oraclePool.prop_javax.net.ssl.keyStoreType=JKS
jdbcService.oraclePool.prop_javax.net.ssl.keyStorePassword=password
```

5. Repeat step 4 for the following Oracle connection pools by changing only the poolname:

- oraclePool_local
- oraclePool_NoTrans
- oracleArchivePool
- oracleUIPool

If you have any other database pools, you will need to add the properties for those pools.

6. Open the `sandbox.cfg` file and change the database connection information to:

```
ORACLE_JDBC_URL= jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(
HOST=<DB host>)(PORT=<TCPS port as configured in DB config section above>))(
CONNECT_DATA=(SERVICE_NAME=<service name>)))
```

7. Navigate to `\install_dir\install\activemq\conf` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. <p>The Administrator: Command Prompt dialog box is displayed.</p>

8. Open the activemqconfig.xml.in file and modify the database connection information:

- Remove or comment out the following default ActiveMQ database configuration information:

```

#:ifdef ORACLE
<bean id="gis-ds" class="org.apache.commons.dbcp.BasicDataSource"
destroy-method="close" singleton="true" lazy-init="default"
autowire="default" dependency-check="default"
SCIOVERRIDEName="persistence-bean">
<property name="driverClassName">
<value>oracle.jdbc.driver.OracleDriver</value>
</property>
<property name="url">
#:ifdef ORACLE_JDBC_URL
<value>&ORACLE_JDBC_URL;</value>
#:else
<value>jdbc:oracle:thin:@&ORA_HOST;:&ORA_PORT;:&ORA_DATA;</value>
#:endif
</property>
<property name="username">
<value>&ORA_USER;</value>
</property>
<property name="password"><value>&ORA_PASS;</value>
</property>
<property name="maxActive"><value>32</value>
</property>
</bean>
#:endif

```

- Add the following ActiveMQ database configuration information:

```

<bean id="gis-ds"
class="oracle.jdbc.pool.OracleDataSource" destroy-method="close"
singleton="true" lazy-init="default" autowire="default"
dependency-check="default">
<property name="URL"><value>&ORACLE_JDBC_URL;</value></property>
<property name="user"><value>&ORA_USER;</value></property>
<property name="password"><value>&ORA_PASS;</value></property>
<property name="connectionProperties"><value>
javax.net.ssl.trustStore: /.../path/.../ClientKeyStore.jks
javax.net.ssl.trustStoreType:JKS
javax.net.ssl.trustStorePassword:password
oracle.net.ssl_version:3.0
javax.net.ssl.keyStore: /.../path/.../ClientKeyStore.jks
javax.net.ssl.keyStoreType:JKS
javax.net.ssl.keyStorePassword: password
driverClassName:oracle.jdbc.driver.OracleDriver
maxActive:32
</value>
</property>
</bean>

```

9. Navigate to `\install_dir\install\bin` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

10. Enter `StartWindowsService.cmd`.

11. Restart Sterling Integrator. All the database connections from Sterling Integrator are now connected through TCPS (encrypted) mode.

Configure Microsoft SQL Server with Sterling Integrator

Microsoft SQL Server Database Configuration Checklist

About this task

You can use an Microsoft SQL Server database for maintaining information in the Sterling Integrator.

Before you begin:

- If you are reinstalling the software, be aware that data in your existing database will be deleted. To prevent this, either back up the existing database or save it under a different name.
- After creating and configuring your database, recycle the database. Then stop and restart to apply the changes.

Use the following checklist to configure Microsoft SQL Server for Sterling Integrator:

#	Microsoft SQL Server Database Configuration Checklist	Your Notes
1	<p>If you do not have Microsoft SQL Server installed, follow the installation procedures in the SQL server installation manual.</p> <p>Refer to the Microsoft SQL server documentation on creating the database, including creating a schema repository, login, and tablespace.</p> <p>Be sure to install the correct version and patches.</p> <p>See <i>System Requirements</i> for supported version information.</p>	
2	<p>For Microsoft SQL 2005, install the Microsoft SQL 2005 Server Service Pack and Hotfix.</p>	
3	<p>Ensure the Microsoft SQL Database parameters are set.</p>	
4	<p>Review the Microsoft SQL Server Database user privileges.</p>	
5	<p>Configure Snapshot for Microsoft SQL Server.</p>	
6	<p>Install the Microsoft SQL Server JDBC driver.</p>	

Microsoft SQL Server Database User Privileges

In Microsoft SQL Server, you must grant DBO (Database Owner) permission to the user. The DB_DDLADMIN role is required for creating objects in the SQL Server database.

Install Microsoft SQL Server 2005 Service Pack and Hotfix

About this task

Before you begin:

- Ensure that Named Pipes & TCP/IP protocols are enabled in the network utility of the SQL Server.
- For SQL Server 2005, do not use case-sensitive column names in the database. Case-sensitive names will prevent the SQL Server 2005 System Management Console from loading.

To install Microsoft SQL Server 2005, Service Pack 2 and hotfixes:

Procedure

1. Install the Microsoft SQL Server 2005 base release.
2. Install the Microsoft SQL Server 2005 Service Pack 2. You can download it from <http://www.microsoft.com/downloads/details.aspx?familyid=D07219B2-1E23-49C8-8F0C-63FA18F26D3A&displaylang=en>.
3. Apply the cumulative hotfix package. You can download it from <http://support.microsoft.com/default.aspx?scid=kb;EN-US;933097>.
4. Apply the GDR2 hotfix. You can download it from <http://support.microsoft.com/kb/934459/>. The Microsoft SQL Server 2005 version is now 9.00.3159.

Microsoft SQL Server Database Parameters

To create a database, ensure that the collation property you select supports all the characters for your database. The following parameter settings are required in your Microsoft SQL Server database:

Parameter	Value
Collation Setting	SQL_Latin1_General_CP850_BIN
Sort order	Binary
Security authentication	SQL Server and Windows
Torn Page Detection	Off

Install the JDBC Driver in Microsoft SQL Server 2005

About this task

Sterling Integrator requires the correct Microsoft SQL Server driver. See *System Requirements* for supported version information.

Go to the Microsoft web site to download the driver and any appropriate patches.

Procedure

1. Download `sqljdbc_version_language.tar.gz` to a temporary directory.
2. To unpack the zipped tar file, navigate to the directory where you want the driver unpacked and type the following command: `gzip -d sqljdbc_version_language.tar.gz`
3. To unpack the tar file, move to the directory where you want the driver installed and type the following command: `tar -xf sqljdbc_version_language.tar`

After the package unpacks, you can find out more information about using this driver by opening the JDBC Help System in the `\absolutePath\sqljdbc_version\language\help\default.htm` file. This will display the help system in your Web browser.

4. When the Sterling Integrator installation asks for the location of the JDBC drivers, specify the extracted jar file created after unpacking the archive (usually named `sqljdbc.jar`). The JDBC driver version is the same as the version of the drivers downloaded from Microsoft.

Configure Snapshot for Microsoft SQL Server

About this task

The snapshot feature in Microsoft SQL Server allows you to view a read-only copy of the database even when it is locked. Configuring the snapshot feature can also reduce deadlocks.

Enter the following command to enable the snap shot feature:

```
ALTER DATABASE db_name SET READ_COMMITTED_SNAPSHOT ON;
```

Database Password Management

Database Passwords

A password is used by the system to connect to its database. The password is stored as clear text in a system property file. If the security policies at your company require you to encrypt these passwords, you can do so after you install the system. Encrypting these passwords is optional.

Database Passwords Encryption Methods

Database passwords are encrypted using one of two methods, `OBSCURED` or `ENCRYPTED`. The encryption method is decided by the value of the `encryptionPrefix` in `propertyEncryption.properties` or `propertyEncryption.properties_platform_security_ext` file.

Encrypt Database Passwords (Windows)

About this task

To encrypt the database password:

Procedure

1. Stop the Sterling Integrator.
2. Navigate to `\install_dir\install\bin` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. <p>The Administrator: Command Prompt dialog box is displayed.</p>

3. Enter `enccfgs.cmd`.

4. Enter `setupfiles.cmd`.
5. Enter `deployer.cmd`.
6. Enter `startWindowsService.cmd` to start the Sterling Integrator.
7. Enter your passphrase.

Decrypt Database Passwords (Windows)

About this task

To decrypt the database password:

Procedure

1. Stop the Sterling Integrator.
2. Navigate to `\install_dir\install\properties` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. <p>The Administrator: Command Prompt dialog box is displayed.</p>

3. Open the `sandbox.cfg` file.
4. Copy encrypted password from the `database_PASS` property.
Use the text that appears after the `database_PASS=` text. For example, if `database_PASS= OBSCURED:123ABCxyz321`, you would copy the text `OBSCURED:123ABCxyz321`. (OBSCURED is the encryption method for the password.)
5. Navigate to `\install_dir\install\bin` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. <p>The Administrator: Command Prompt dialog box is displayed.</p>

6. Enter `decrypt_string.cmd` encrypted `_password`.
For `encrypted_password`, use the text that you copied in Step 4.
You are prompted for the Sterling Integrator passphrase.
Your decrypted password appears.
7. Navigate to `\install_dir\install\properties` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

8. Edit the sandbox.cfg file to replace the encrypted password with the password that was returned in Step 6.
9. You need to decrypt the entries for YANTRA_DB_PASS and DB_PASS. Repeat Steps 4 to 8 to decrypt these entries. You should also decrypt any passwords present in the property files. Encrypted passwords typically reside in the following property files:
 - sandbox.cfg
 - apservsetup
 - jdbc.properties/.in
 - customer_overrides.properties/.in
10. Navigate to `\install_dir\install\bin` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

11. Enter `setupfiles.cmd`.
12. Enter `deployer.cmd`.
13. Enter `startWindowsService.cmd` to start the Sterling Integrator.

Chapter 4. Install the Software

General Installation/Upgrade Information for a Windows Cluster Environment

Caution: Sterling Integrator should be installed behind a company firewall for security purposes. See the Perimeter Server and Security topics in the Sterling Integrator documentation library for more information on secure deployment options.

Use one of the following methods to install your system:

- GUI method
- Silent Installation method

The cluster environment does not support the following items:

- MySQL database
- AS2 Edition

The following are some general installation guidelines:

- The installation directory must not already exist because the installation process creates it.
- The installation directory must have adequate free disk space.
- The name of the directory cannot include spaces and must be less than 30 characters long excluding separators. Using a directory name of more than 30 characters could create an install that is impossible to delete. An example of an installation directory is C:\SI_50\install_dir\install.
- All nodes must use the same database.
- All nodes must use the same passphrase.
- All nodes must use the same operating system.
- When installing nodes on different machines, the initial port numbers must be the same. Installing nodes on different machines helps you take advantage of cluster features such as, reliability, availability, scalability, and failover.
- When installing nodes on the same machine, you must install node 2 and higher in different directories. Each initial port must be at least 200 higher or lower than the initial port for the other nodes.
- If you need to install more than one instance of Sterling Integrator on the same Windows server, you must install the second instance in a different directory.
- Clustering is not supported for systems that use the MySQL database.
- Sterling Integrator 5.1 does not support IPv6 installation on Windows. Before applying an IPv6 address, see the *IPv6 Capabilities* section in Sterling Integrator 5.1 *System Requirements* guide.

General Installation Wizard Information for Windows

The installation wizard provides:

- The option of either entering the paths or selecting the paths and files (**Select File**).

- For every screen in the GUI-Based installation wizard, you need to click **Next** to move to the next step the wizard. The click **Next** step is not represented in each step in the procedure.

Install Sterling Integrator (Windows Cluster)

About this task

Before you begin:

- You should have completed the Preinstallation Checklist.
- The license file must reside on the host machine on which the application is being installed. If you saved the license file to a Windows client, transfer the license file to the host.
- Sterling Integrator 5.1 does not support IPv6 installation on Windows. Before applying an IPv6 address, see the *IPv6 Capabilities* section in Sterling Integrator 5.1 *System Requirements* guide.
- *install_dir* refers to the installation directory where the software is installed. Do not use any pre-existing directory name or an old version of the Sterling Integrator installation directory. If you do, you could inadvertently overwrite the existing installation.
- *parent_install* refers to the parent directory of the installation directory that you create during the installation.
- If you are installing Sterling Integrator on VMware, provide the IP address of the virtual machine, not the IP address of the VMware host. For example, if 10.251.124.160 is the IP address of the VMware host and 10.251.124.156 is the IP address of the Windows 2003 server it is hosting, you should use 10.251.124.156 as the correct IP address to install Sterling Integrator.
- The installation creates subsequent ports based on the initial port number. For all of the port assignments, see the `\install_dir\install\properties\sandbox.cfg` file.

To install Sterling Integrator:

Procedure

1. Close all open Windows programs and any command prompt windows.
2. From the installation media, copy `SCIInstallWizard.jar` and `SI.jar` to your desktop.
3. To start the installation, use one of the follow methods:

For Windows Server 2003 or earlier	For Windows Server 2008
<ul style="list-style-type: none"> • Open a command prompt window (from the Run dialog box). • Enter <code>\path_to_java\bin\java -jar \absolutePath\SCIInstallWizard.jar</code> 	<p>Complete the following steps:</p> <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed. • Enter <code>\path_to_java\bin\java -jar \absolutePath\SCIInstallWizard.jar</code>

The installation dialog box appears.

4. Click **Next** to start the installation program.
5. Review the License conditions and click **Accept** to accept the terms.

6. Enter the **full path to the JDK** directory.
7. Enter the **full path to the license file**.
If you have not installed a license file, you can minimize this window, obtain the license file, and then return to the installation process.
8. Enter the **full path to your JCE** file.
9. Enter the path to installation directory. If the directory does not exist, click **Yes** at the prompt *The directory does not exist, create it?*.
The installer creates the installation directory. This installation directory is referred to as *install_dir*. Below the installation directory, the installer creates a directory named *install*. This directory contains the installation files.
10. Enter the path to the install jar file (SI.jar).
11. Enter the **explicit IP address** for the server or use the default value of localhost.
12. Enter the **initial port number** or use the default value of 8080.
13. Enter your system **passphrase**.
14. Re-enter the system **passphrase**.
15. Enter the **administrative e-mail address** to which you want system alert messages sent.
16. Enter the **SMTP mail server** (IP address or host name) that you want to use for system alert messages and other administrative notices.
17. If you want to enable **FIPS** (Federal Information Processing Standards) mode, select the checkbox. The default is disable FIPS mode.
18. Select the database that you want to use (Oracle, Microsoft SQL Server, or DB2).
19. Select all options that apply to this node:

Choices:	Action
This installation is an upgrade from a prior version.	Do not select this option.
This installation is for a cluster node 2 or higher	<ul style="list-style-type: none"> • For node 1: Do not select the check box. • For node 2 or higher: Select the check box.

Choices:	Action
<p>(Skip for MySQL)</p> <p>Apply database schema automatically?</p>	<ul style="list-style-type: none"> • If yes, no action required. The default is to automatically apply the DDL statements. • If you want to manually create the database schema, then clear the Apply database schema automatically check box. After the installation wizard stops, you must perform these additional steps: <ol style="list-style-type: none"> 1. Manually create the database schema. 2. Rename or delete the <i>install_dir</i> directory. 3. Start the installation wizard again. <p>When you are executing the scripts, it is important to execute the SQL scripts in a particular order. The SQL script order is dependant on the database configured with your system. See the database documentation for further information.</p> <p>Important: In version 5.1 of Sterling Integrator, there is an issue with this feature and the installation wizard. For information on the corrective workaround, see InQuira Article NFX11576.</p>
<p>Verbose install?</p>	<ul style="list-style-type: none"> • By default, the check box is not selected. • Select the checkbox to generate the installation log. The events that occur during the installation are recorded in InstallSI.log file.

20. Enter the database connection information.

- Database user name
- Database password (and confirmation)
- Database catalog name
- Database host name
- Database port
- (Oracle and Microsoft SQL Server only) Absolute path and file name for one JDBC driver file
- (DB2 only) Absolute paths and file names for two JDBC driver files

Use the Type-4 JDBC driver. This type of driver converts JDBC calls into the network protocol used directly by DB2, allowing a direct call from the Sterling Integrator to the DB2 server.
- (Oracle only) Select the check box to select the data type to use for caching. Select either the default BLOB (binary large object) columns data type or the Long Raw data type.

You can significantly improve performance by enabling the cache on the BLOB data object in Oracle. For more information, refer to the Sterling Integrator documentation for slow performance in Oracle.

21. Review and confirm the database information.

22. Review the default **Install Actions**. The following check boxes are automatically selected and you can not clear them:

- Verify Operating System is supported

- Verify the selected JDK is supported
 - Install Components
 - Save install files
 - Clean Up Files
 - Install Windows Service
23. If you want to **Create Desktop Icons (Windows & Linux)**, click **Next**. By default, the check box is selected. If you created the desktop icon and are using Windows Server 2008, you need to complete the *Configure the Desktop Icon for Windows Server 2008* task after the installation is complete.
24. Click **Next** to continue.
The Installation Progress screen appears. You can click **Show Details** to confirm your installation information before starting the installation.
25. Click **Install**.
The Installation Progress screen shows the general progress of the installation through different stages. For more information about these stages, click **Show Details**.
For more detailed information about the installation, refer to the `\install_dir\PreInstallSI.log` file. The installation completes automatically. When the installation is finished, the system displays a dialog box with the message Installation Wizard completed. Please see the installation guide for next steps.
Installation information is in the following files:
- ant.install.log (in the `install_dir` directory)
 - InstallSI.log (in the `\install_dir\install` directory)
26. To install each additional node, navigate to your working directory, and using one of these methods:

For Windows Server 2003 or earlier	For Windows Server 2008
<ul style="list-style-type: none"> • Open a command prompt window (from the Run dialog box). • Enter <code>\path_to_java\bin\java -jar \absolutePath\SCIInstallWizard.jar</code> 	Complete the following steps: <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed. • Enter <code>\path_to_java\bin\java -jar \absolutePath\SCIInstallWizard.jar</code>

The installation dialog box appears. The program verifies support for your operating system and JDK. It also verifies that your operating system is patched to the required level. You will follow the same steps as you did for node 1 until you get to Step 19. When prompted, **This installation is for a cluster node 1 or higher**, enter **true**.

27. If you installed multiple nodes on the same machine or used different base ports for node 2 onward, you need to complete the following additional steps:

Step	Action	Your Notes
1	Navigate to <code>\install_dir\install\properties</code> for node 1.	
2	In the <code>noapp.properies_platform_ifcresources_ext</code> file, record the value for <code>multicastBasePort</code> .	

Step	Action	Your Notes
3	In the <code>jgroup_cluster.properties</code> file, record the values for the <code>mcast_port</code> parameters of the <code>property_string</code> and <code>lock.protocolStack</code> properties.	
4	For each subsequent node, you need to perform the remaining steps.	
5	Navigate to <code>\install_dir\install\properties</code> for each node (node 2 and higher).	
6	In the <code>noapp.properies_platform_ifcresources_ext.in</code> file, update the value of the <code>multicastBasePort</code> to match the value for node 1. For example, replace the string <code>&MULTICAST_NODE_PORT1;</code> with the port number 45460: <ul style="list-style-type: none"> • (before) <code>multicastBasePort=&MULTICAST_NODE_PORT1;</code> • (after) <code>multicastBasePort=45460</code> 	
7	In the <code>jgroups_cluster.properties.in</code> and <code>jgroups_cluster.properties_fifo_ext.in</code> files, update all occurrences of <code>mcast_port</code> to match the values for node 1.	
8	After you have updated the attributes for all of the nodes, enter: <code>\install_dir\install\bin\setupfiles.cmd</code> for node 2 and higher.	

28. Determine if you need to apply any maintenance patches to the installation. Refer to *Installation Maintenance* to get information on how to install the latest patch.

Silent Installation

The silent installation method automates part of the installation process and limits your manual interaction with the installation program. To use the silent installation method, you will need to first create a silent install file using a text editor.

Create the Silent Installation File (Windows Cluster)

About this task

The following entries correlate to prompts in the Install Using the GUI-Based method procedure. Create a silent installation file with the following variables:

Entry	Description
ACCEPT_LICENSE	(Required) Indicates if the user accepts the license agreement. Default: YES
JVM_LOC	(Required) Full path to JDK directory.
LICENSE_FILE_PATH	(Required) Full path to a valid license file. Example: <code>\absolutePath\Full_License.xml</code>
SI_LICENSE_AVAILABLE	(Optional) Indicates if a license is being passed in and is required for the installation. Default: YES

Entry	Description
JCE_DIST_FILE	(Required) Full path to unlimited strength JCE policy file. If present, this file will overwrite the JCE file in the JDK. Example: <code>\absolutePath\unrestrict123.zip</code>
INSTALL_DIR	(Required) Directory that includes the bin subdirectory (where many commands are stored) and the properties subdirectory (where many properties are stored).The INSTALL_DIR property cannot point to a pre-existing directory, or the installation will fail. It can include the following: <ul style="list-style-type: none"> • The installation directory that you specify during an interactive installation. • The subdirectory “install”. Although you can enter your own path, the <code>\install_dir\install</code> path matches the path that is created during an interactive installation.
REINIT_DB	(Required) Indicates if database should be initialized. <ul style="list-style-type: none"> • For node 1 of a cluster, this property is true. • For node 2 and higher of a cluster, this property is false. Default: true
CLUSTER	(Required) Indicates if this is the second or higher node of a cluster installation. Valid values: <ul style="list-style-type: none"> • true - This is the second or higher node of a cluster installation. • false (default) - This is the first node of a cluster or a single node (non-cluster) installation.
INSTALL_IP	(Required) Host name or IP address. Valid values: <ul style="list-style-type: none"> • localhost (default) • Your IP address or host name If you are installing Sterling Integrator on VMware, provide the IP address of the virtual machine, not the IP address of the VMware host. For example, if 10.251.124.160 is the IP address of the VMware host and 10.251.124.156 is the IP address of the Windows 2003 server it is hosting, you should use 10.251.124.156 as the correct IP address to install Sterling Integrator. Note: Sterling Integrator 5.1 does not support IPv6 installation on Windows. Before applying an IPv6 address, see <i>IPv6 Capabilities</i> section in <i>System Requirements</i> guide. You must install using a host name, not an IPv6 address, otherwise the Lightweight JDBC adapter and Graphical Process Modeler (GPM) will not work.
PORT1	(Required) Base port for ASI server. Ports are assigned consecutively from this port. Example: 12345 Default: 8080
APSERVER_PASS	(Required) Passphrase used to secure all encrypted data in database.
SI_ADMIN_MAIL_ADDR	(Required) E-mail address for the administrative user. Example: abc@xyz.com

Entry	Description
SI_ADMIN_SMTP_HOST	(Required) Valid SMTP host through which the system can e-mail the administrative user. Example: mail.xyz.com
FIPS_MODE	(Optional) Indicates if you are using FIPS (Federal Information Processing Standards) mode. Valid values: <ul style="list-style-type: none"> • true - Enable FIPS mode. • false (default) - Disable FIPS mode.
DB_VENDOR	(Required) Database vendor. Valid values: <ul style="list-style-type: none"> • Oracle • MSSQL2005 (use this value for Microsoft SQL 2005 and 2008) • DB2 • MySQL (default)
DB_CREATE_SCHEMA	(Required) Indicates if you want the database schema automatically created. Valid values: <ul style="list-style-type: none"> • true (default) - Automatically create the schema. • false - Manually create the schema. <p>If you create the database schema manually, restart the installation procedure in a new installation directory. You can delete the installation directory created earlier.</p>
DEBUG	(Optional) Records events that occur during the installation in InstallSI.log file. Valid values: <ul style="list-style-type: none"> • true - records events that occur during the installation. • false (default) - does not record the events that occur during installation.
DB_USER	(Required) Database user name. Example: abcd_123_1
DB_PASS	(Required) Database password. Example: xyz
DB_DATA	(Required) Database catalog name. Example: abcd
DB_HOST	(Required) Database host name. Example: abcd Default: localhost
DB_PORT	(Required) Database port. Example: 1234

Entry	Description
DB_DRIVERS	<p>(Required) Full path to JDBC driver files. If DB_VENDOR is:</p> <ul style="list-style-type: none"> • Oracle or MSSQL, specify one driver. • DB2, specify two drivers. <p>If you specify more than one driver, use colons (:) to separate the file names.</p> <p>Examples:</p> <ul style="list-style-type: none"> • <code>JDBC_driver_dir\db2jdbc.jar</code> • <code>JDBC_driver_dir\db2_1_jdbc.jar;JDBC_driver_dir\db2_2_jdbc.jar</code>
ORACLE_USE_BLOB	<p>(Required if DB_VENDOR=Oracle) Indicates the data type to use for caching.</p> <ul style="list-style-type: none"> • true (default) - BLOB (binary large object) • false - Long Raw
MSSQL2005	<p>(Required for Microsoft SQL Server 2005) This attribute is case-sensitive.</p> <ul style="list-style-type: none"> • Set this attribute to the default value of true. • (All other servers) Do not include this attribute.
JDK64BIT	<p>(Optional) Indicates if a 32-bit or 64-bit JDK is being used. Refer to the <i>System Requirements</i> to determine the type of JDK for your operating system.</p> <p>Valid values:</p> <ul style="list-style-type: none"> • true (default) - 64-bit • false - 32-bit
Icons	<p>(Required) Indicates whether to create a desktop icon for accessing Sterling Integrator.</p> <p>Valid values:</p> <ul style="list-style-type: none"> • true - Create a desktop icon. • false (default) - Do not create a desktop icon. <p>If you created the desktop icon and are using Windows Server 2008, you need to complete the <i>Configure the Desktop Icon for Windows Server 2008</i> task after the installation is complete.</p>

The following entries do not directly correlate to prompts in the installation procedure. Use these entries to customize or document your installation.

Entry	Description
DB_DRIVERS_VERSION	<p>(Optional) Free form version string for JDBC driver. This is informational only.</p> <p>Example: 8_1_5</p>
LOAD_FACTORY_SETUP	<p>(Optional) Indicates whether factory setup should be loaded during installation. To manually set LOAD_FACTORY_SETUP to false after an installation where LOAD_FACTORY_SETUP=true (the default value), change LOAD_FACTORY_SETUP to false in sandbox.cfg file.</p> <p>Valid values:</p> <ul style="list-style-type: none"> • true (default).- loads factory setup during installation. • false - does not load factory setup during installation. Run loadDefaults command after installation.
CONFIG_GS	<p>(Optional) Indicates whether integration with Gentrans Server should be configured.</p> <p>Default: No</p>

Entry	Description
NO_DBVERIFY	(Optional) Valid values are true or false. When set to true during installation and installservice, dbverify will not be run. This means that the Sterling Integrator will not generate DDL to make the database like the XML entity repository.

Install Sterling Integrator Using a Silent Installation File (Windows Cluster)

About this task

Sterling Integrator 5.1 does not support IPv6 installation on Windows. Before applying an IPv6 address, see the *IPv6 Capabilities* section in Sterling Integrator 5.1 *System Requirements* guide.

Before you begin, you should have already created the silent install file.

To install Sterling Integrator in windows cluster environment using a silent installation file:

Procedure

1. From the installation media, copy SI.jar to a Windows directory.
2. Set up your silent installation file and record its location.
3. To start the installation, use one of the follow methods:

For Windows Server 2003 or earlier	For Windows Server 2008
<ul style="list-style-type: none"> • Open a command prompt window (from the Run dialog box). • Enter <pre>\absolutePath\bin\java -Xmx512m -jar \absolutePath\SI.jar -f \absolutePath\SilentInstallFile</pre> 	<p>Complete the following steps:</p> <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed. • Enter <pre>\absolutePath\bin\java -Xmx512m -jar \absolutePath\SI.jar -f \absolutePath\SilentInstallFile</pre>

The installation begins. The program verifies support for your operating system and JDK. You can follow the progress of the installation on screen.

When the installation is finished, the system displays the following message:
Installation has completed successfully.

Important: Windows services are not installed during a silent installation. After the installation completes, you must go to `\install_dir\bin\` and run `installwindowsServices.cmd`

4. (Skip this step if you are applying database schema automatically.) If you are going to manually create the database schema, the installation will stop. After it has stopped, you need to perform the following steps:
 - a. Manually create the database schema.
 - b. Rename or delete the `install_dir` directory.

c. Start the silent installation again.

When you are executing the scripts, it is important to execute the SQL scripts in a particular order. The SQL script order is dependant on the database configured with your system. See the database documentation for further information.

Important: In version 5.1 of Sterling Integrator, there is an issue with this feature and the installation wizard. For information on the corrective workaround, see InQuira Article NFX11576.

5. If you are installing nodes on separate machines, copy the silent install file for node 1 into a new silent install file and then set REINIT_DB=false and set CLUSTER=true. This REINIT_DB=false prevents the database from being re-initialized. After you have the silent install files for node 2 and higher, proceed to Step 8.
6. If you are installing multiple nodes on the same machine, copy the silent install file for node 1 into a new silent install file and then set REINIT_DB=false, set CLUSTER=true, use a different installation directory for each node (INSTALL_DIR) and make sure that the initial port for each node is 100 port numbers higher or lower than node 1. After you have the silent install files for node 2 and higher, proceed to Step 8.
7. To start the installation of nodes 2 and higher of the cluster:

For Windows Server 2003 or earlier	For Windows Server 2008
<ul style="list-style-type: none"> • Open a command prompt window (from the Run dialog box). • Enter <pre>\absolutePath\bin\java -jar \absolutePath\SI.jar -f \absolutePath\SilentInstallFile - cluster</pre> 	<p>Complete the following steps:</p> <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed. • Enter <pre>\absolutePath\bin\java -jar \absolutePath\SI.jar -f \absolutePath\SilentInstallFile - cluster</pre>

8. If you installed multiple nodes on the same machine or used different base ports for node 2 onward, you need to complete the following additional steps:

Step	Action	Your Notes
1	Navigate to <code>\install_dir\install\properties</code> for node 1.	
2	In the <code>noapp.properies_platform_ifcresources_ext</code> file, record the value for <code>multicastBasePort</code> .	
3	In the <code>jgroup_cluster.properties</code> file, record the values for the <code>mcast_port</code> parameters of the <code>property_string</code> and <code>lock.protocolStack</code> properties.	
4	For each subsequent node, you need to perform the remaining steps.	
5	Navigate to <code>\install_dir\install\properties</code> for each node (node 2 and higher).	

Step	Action	Your Notes
6	<p>In the <code>noapp.properties_platform_ifcresources_ext.in</code> file, update the value of the <code>multicastBasePort</code> to match the value for node 1.</p> <p>For example, replace the string <code>&MULTICAST_NODE_PORT1;</code> with the port number 45460:</p> <ul style="list-style-type: none"> • (before) <code>multicastBasePort=&MULTICAST_NODE_PORT1;</code> • (after) <code>multicastBasePort=45460</code> 	
7	<p>In the <code>jgroups_cluster.properties.in</code> and <code>jgroups_cluster.properties_fifo_ext.in</code> files, update all occurrences of <code>mcast_port</code> to match the values for node 1.</p>	
8	<p>After you have updated the attributes for all of the nodes, enter:</p> <p><code>\install_dir\install\bin\setupfiles.cmd</code> for node 2 and higher.</p>	

- Determine if you need to apply any maintenance patches to the installation. Refer to *Installation Maintenance* to get information on how to install the latest patch.

Configure the Sterling Integrator Desktop Icon for Windows Server 2008

About this task

User Access Control (UAC) is a security component in Windows Server 2008. If you enable the UAC, it affects the installation process and the daily processing for Sterling Integrator. If you disable the UAC, which requires a reboot, the installation process and daily processing for Sterling Integrator remains the same as in previously supported Windows version.

If you installed or upgraded the Sterling Integrator on a Windows Server 2008 and you created a desktop icon for Sterling Integrator, you must complete this task in order for the desktop icon to work.

Procedure

- Right-click on the Sterling Integrator **desktop icon**.
- Click **Properties**.
- In the Shortcut tab, click **Advanced**.
- Select the check box for **Run as Administrator**.
- Click **OK** to apply the changes to Advanced Properties.
- Click **OK**.

Chapter 5. Validate the Installation

Validate the Installation Checklist in a Cluster Environment

As part of the installation, you need to run the following tests to ensure that the software installation was successful. Complete the following tasks:

#	Validate Installation Task	Completed
1	Verify the Cluster Environment Settings in Property Files.	
2	Configure the Nodes in the Cluster.	
3	Start a Cluster.	
4	Access Sterling Integrator.	
5	Validate the Installation.	
6	Verify the Cluster is Running from the User Interface.	
7	Stop a Node (Hard Stop or Soft Stop) or Stop the Cluster.	

Verify the Cluster Environment Settings in Property Files

About this task

To verify the cluster environment is correct, check these property settings on node 2:

Procedure

1. Verify that CLUSTER=true is in the sandbox.cfg property file.
2. Verify that CLUSTER=true is in the centralops.properties property file.
3. Verify that CLUSTER=true is in the noapp.properties property file.
4. Verify that cluster_env property=true is in the ui.properties property file.

Configure the Nodes in Windows Cluster

About this task

The first time you configure a cluster, you need to use the startCluster command with true option (startCluster.cmd nodeName true). Initial configuration should be the only time you need to use the startcluster command. However, if you should need to use the command again, use the startcluster command with the false option (startCluster.cmd nodeName false). The false option prevents any configuration changes from affecting the system, especially after installation of a patch or hot fix.

To configure the nodes in a Windows cluster environment, you need to perform the following task for each node, starting with node 1:

Procedure

1. Navigate to `\install_dir\install\bin` for the node using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

2. Enter `startCluster.cmd <nodeNumber> <true or false>`. Where `<nodeNumber>` is the number of the node, `true` performs database updates and `false` prevents database updates. For example for node 1, enter `./startCluster.cmd 1 true`.
3. Enter `startWindowsService.cmd`. Perform this step for each node. The final startup processes run, concluding with the following message: Open your Web browser to `http://host:port/dashboard` where `host:port` is the IP address and port number on your system.
4. Record the URL address so that you can access Sterling Integrator.

Access Sterling Integrator

About this task

To log in to Sterling Integrator:

Procedure

1. Open a browser window and enter the address displayed at the end of startup. The login page displays.
2. Enter the default user ID (`admin`) and password (`password`). The default login is at an administrative level. One of your first tasks as an administrator is to change the administrative password and to register other users with other levels of permission.

Validate the Installation

About this task

Validate the installation by testing a sample business process:

Procedure

1. From the Administration Menu, select **Business Process > Manager**.
2. In the Process Name field, enter `Validation_Sample_BPML` and click **Go!**
3. Click **execution manager**.
4. Click **execute**.
5. Click **Go!** The Status: Success message displays in the upper left side of the page.

Stop a Node in the Windows Cluster Configuration (Hard Stop)

About this task

You can stop a single node Sterling Integrator in a Windows cluster environment. To run a hardstop, perform this task for each node:

Procedure

1. Navigate to `\install_dir\install\bin` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none">• Click Start.• Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

2. Enter `hardstop.cmd`.
3. Enter your passphrase. You can also perform this task by selecting **Operations > System > Troubleshooter**. Then click the **shutdown** link for the node you want to stop.

Stop Sterling Integrator (Windows Cluster)

About this task

To stop the entire cluster in a Windows environment:

Procedure

1. From the Administration Menu, select **Operations > System > Troubleshooter**.
2. Click **Stop the System** and wait for shutdown to complete.

Stop Sterling Integrator (Hardstop Windows)

About this task

To stop Sterling Integrator in a Windows environment:

Procedure

1. Navigate to `\install_dir\install\bin` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none">• Click Start.• Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

2. Enter `hardstop.cmd`. You should receive a message that services have been stopped. Services include Noapps, Opsserver, WebDav, and Database-related service.

Stop Cluster (Softstop Windows)

About this task

Soft stop in a cluster environment suspends all scheduled business processes. It is recommended to run the `hardstop` command on each of the nodes.

To soft stop the cluster:

Procedure

1. Navigate to `\install_dir\install\bin` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none">• Click Start.• Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

2. Enter `softstop.cmd`. You should receive a message that services have been stopped. Services include Noapps, Opsserver, WebDav, and Database-related service.

Restart the Windows Cluster

About this task

To restart the entire cluster in a Windows environment:

Procedure

1. Navigate to `\install_dir\install\bin` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none">• Click Start.• Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

2. Enter `startWindowsService.cmd restart`.

What to do next

Note: If you need to release all the locks in a cluster and both nodes are down, use the restart parameter for Node 1. For example:

For Node 1, enter:

```
startWindowsService.cmd restart
```

For Nodes 2 and higher, enter:

```
startWindowsService.cmd
```

Chapter 6. Post Installation Configuration

Post Installation Configuration Checklist for Cluster Environment (Windows)

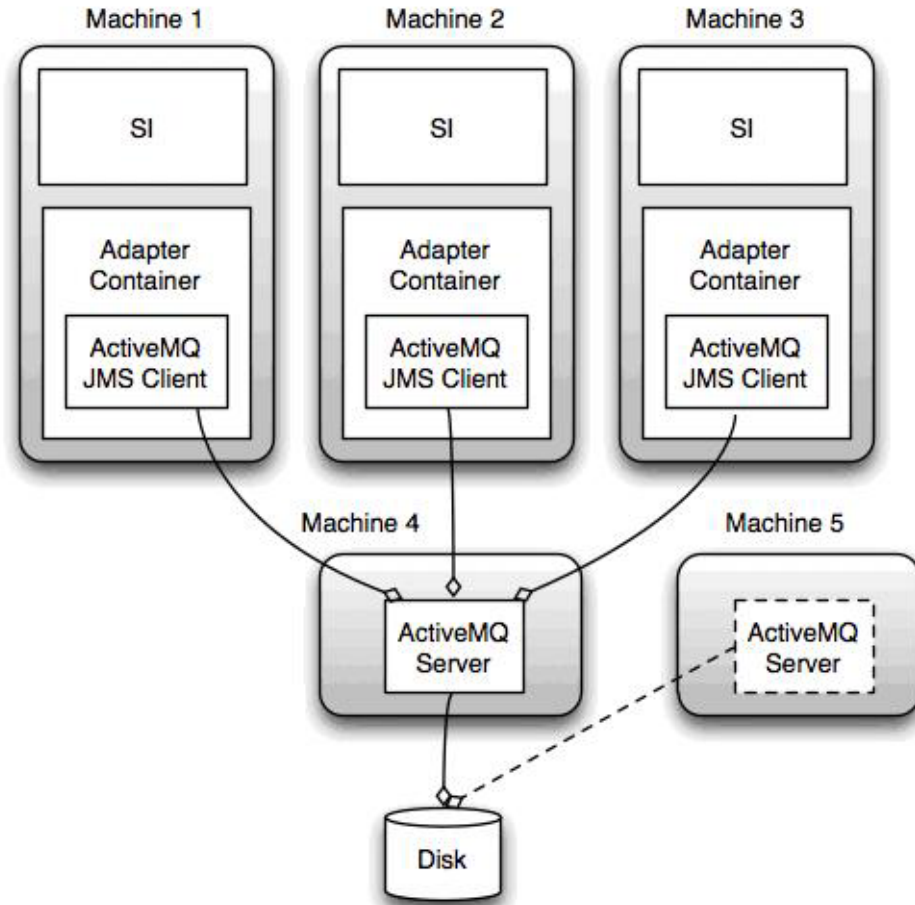
After you have installed the Sterling Integrator, you need to complete the post installation configuration checklist. Review all of the tasks, but note, some tasks may not be required for your system installation.

#	Post Installation Configuration Checklist	Your Notes
1	For security purposes, change the default user ID passwords immediately after the installation is completed. See the <i>Update My Account Information</i> task in the documentation library.	
2	Configure ActiveMQ for a cluster environment.	
3	Download Sterling Integrator Tools.	
4	Determine if you need to modify any Property Files.	
5	Configure Shared File System as Document Storage.	
6	Add host[port] from all the nodes to the jgroups_cluster.property.in for each node.	
7	Configure Customer Overrides File with a Firewall between Nodes.	

JMS Cluster Configuration for Failover

To allow proper JMS execution and failover in the Sterling Integrator 5.1 cluster environment, you must configure an external ActiveMQ using the *Configure ActiveMQ for a Cluster Environment* task.

The following diagram illustrates how the ActiveMQ can be configured to increase availability and failover.



Configure ActiveMQ for a Cluster Environment (Windows)

About this task

To configure ActiveMQ for the windows cluster environment:

Procedure

1. Download the ActiveMQ 5.2 from <http://activemq.apache.org/activemq-520-release.html> for the appropriate OS.
2. Deploy an instance of ActiveMQ 5.2. This can be on the same machine as Sterling Integrator or on a separate machine.
3. Navigate to `\install_dir\install\properties` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. <p>The Administrator: Command Prompt dialog box is displayed.</p>

4. Copy the `activemq.xml` file to the AMQ conf directory. This file configures the ActiveMQ to:
 - Use failover clustering,
 - Use the SI database for storage
 - Configures the AMQ port usage

By default, ActiveMQ is configured to listen at the Sterling Integrator base port + 64 and the ActiveMQ interface will be at base port + 65 (`http://server:base port + 66/admin`). The port can be changed by editing the config file directly.

5. Navigate to `\install_dir\install\properties` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

6. On each Sterling Integrator application node and each Sterling Integrator container node, the queue configuration must be re-directed to utilize the ActiveMQ cluster. In each node, add the following to the `customer_overrides.properties`:

For FIFO Processing:

```
fifo.broker.username=
fifo.broker.password=
fifo.broker.url=failover:(tcp://amq_master_hostname:amq_master_port,
tcp://amq_slave_hostname:amq_slave_port)
```

For adapters running in separate JVM containers:

```
iwfcqueue.username=
iwfcqueue.password=
iwfcqueue.protocol_config=failover:(tcp://amq_master_hostname:amq_master_port,
tcp://amq_slave_hostname:amq_slave_port)
```

7. Start the ActiveMQ instances. To start ActiveMQ, it is necessary to supply the `activemq.hostname` property with the hostname for the current system. For example:

```
activemq.bat -Dactivemq.hostname=ExampleHostname
```

See <http://activemq.org> for additional information about running an ActiveMQ instance.

8. Start Sterling Integrator.

Download Sterling Integrator Tools

Sterling Integrator includes tools that run on a desktop or personal computer. After you install, you can install the following tools:

- Map Editor and associated standards
- Graphical Process Modeler (GPM)
- Web Template Designer
- (If licensed) MESA Developer Studio plug-ins, including, MESA Developer Studio Software Development Kit (SDK) and MESA Developer Studio Skin Editor

- If licensed) Reporting Services, which requires MESA Developer Studio if you want to use the plug-ins to create fact models and custom reports.

Conflicting IP addresses can cause problems when you download a desktop tool.

Property Files Configuration in a Windows Environment

Property files contain properties that control the operation of the Sterling Integrator. For example, the REINT_DB property in the sandbox.cfg file controls whether or not a database is initialized when you install Sterling Integrator.

By modifying the values of these properties, you can customize the Sterling Integrator to suit your business and technical needs. Most property files are in the `\install_dir\install\properties` directory.

After installing the Sterling Integrator, most property files and scripts do not need any further configuration for basic operation. However, if you want to customize any specific operations, for example setting a different logging level - you will need to edit (or in some cases, create) certain property or .xml files.

Before changing any property files, refer to Working with Property Files documentation for general information about how to work with Property Files.

Areas where you might need to make specific property files changes after an installation include:

- LDAP user authentication
- Prevention of cross-site script vulnerabilities
- Logging configuration
- Process-specific property file settings
- Securing the Interop Servlet

Configure Shared File Systems as Document Storage (Windows Cluster)

About this task

To configure the shared file systems as document storage:

Procedure

1. Navigate to `\install_dir\install\properties` for the node using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

2. Open the `jdbc.properties.in` file.
3. Update the value of the `document_dir` attribute to point to the shared files system directory where you store documents.

4. Save and close the file.
5. Navigate to `\install_dir\install\bin` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. <p>The Administrator: Command Prompt dialog box is displayed.</p>

6. Enter `setupfiles.cmd`.
7. Restart the Sterling Integrator.

Add host[port] From all the Nodes to the `jgroups_cluster.property.in` for Each Node

About this task

Complete this task for both vertical and horizontal clusters. You will need to complete this task for each node, starting with node 1.

Before you begin, it is important to note that you should never override `mcast_addr` in the `jgroup_cluster.properties`.

To add the host [port] to the `jgroups_cluster.property.in` file:

Procedure

1. Navigate to the `properties` file directory for the node.
2. Determine the `initial_hosts` port for each node:
 - Navigate to the `properties` file directory for the node.
 - Find the `initial_hosts` from the `jgroups_cluster.property` (`initial_hosts=host{port}`).
 - Record the value from the `initial_hosts` for each node.
3. Open the `jgroups_cluster.property.in` file.
4. Add the `initial_hosts` property to the file. For example, if node 1 is on `host1` and node 2 is on `host2`. For node 1, you would add:

```
initial_hosts=host1[port1],host2[port2]
```

For node 2, you would add:

```
initial_hosts=host2[port2],host1[port1]
```
5. Save and close the file.

Services and Adapters Associated with Node 1 in a Cluster

The following service and adapters are associated with node 1 in the cluster:

- Schedule
- FileSystem
- CmdLine
- CDServerAdapter
- CDAdapter

- CDRequesterAdapter
- CEUAdapter
- HttpServerAdapter
- B2B_HTTP_COMMUNICATIONS_ADAPTER
- HTTP_COMMUNICATIONS_ADAPTER
- HTTPClient Adapter
- FTPClientAdapter
- FtpServerAdapter
- SFTPClientAdapter

The following services have storage set to database:

- HttpServerAdapter
- CEUAdapterServiceType
- CDSERVER_ADAPTER

The default storage for all of the workflows is set to database.

Configure Customer Overrides File with a Firewall between Nodes

About this task

If you have configured a firewall between nodes that blocks ports outside of the port range assigned to Sterling Integrator, perform the following task on all nodes:

Procedure

1. Navigate to the Sterling Integrator installation directory.
2. Navigate to the properties directory and locate (or create, if necessary) the customer_overrides.properties file.
3. Open the customer_overrides.properties file using a text editor.
4. Add the following properties:

```
noapp.jnp_host= <host_name>
noapp.jnprmiport=<port_number_1>
noapp.jnprmiport2=<port_number_2>
noapp.useSocketFactories=true
noapp.jndirmiport=<port_number_3>
ops.jnp_host= <host_name>
ops.jnprmiport=<port_number_1>
ops.useSocketFactories=true
ops.jndirmiport=<port_number_2>
ops.jnprmiport2=<port_number_3>
```

This increases the number of threads used by the system.

5. Save and close the customer_overrides.properties file.
6. Stop Sterling Integrator and restart it to apply the changes.

Chapter 7. Installation Maintenance

Installation Maintenance for a Windows Cluster Environment

From time to time, you will need to apply either a patch or a hotfix to your Sterling Integration installation:

- All nodes in the cluster must be patched to the same level. You must stop all nodes in the cluster before installing a patch, then install the patch on each node. Attempting to apply a patch while part of the cluster is running should only be done with the advice of Sterling Commerce Customer Support.
- Patches contain cumulative fixes for a specific version of Sterling Integrator. Because each patch contains the fixes from previous patches, you only need to install the most recent patch. You should periodically check the web site to verify that you have the most recent patch.
- Hot-fix is one or more fixes applied to a specific existing patch.

It is possible to apply patches to nodes while other nodes are processing. However a patch containing any of the following, requires the entire cluster to be down:

- Critical cluster functionality
- Engine-related changes
- Changes to the database

You can preserve your custom changes to system resources (like workflow definitions and maps) when you update your system. During updates, the system can identify when you make a custom change versus when the system makes a change through an upgrade or patch.

When a patch, installation or upgrade is performed, a baseline record of system resources is created. This baseline is not affected by any subsequent customer changes. When another patch is installed, the resources in this baseline are compared to the resources in the existing system. If a baseline and existing resource are not the same, it means that the existing resource was customized and is not overwritten by the patch.

During an update, the baseline is updated with new system resource information, but not with custom changes to resources.

Determine If You Need to Apply a Maintenance Patch (Windows)

About this task

Patches contain cumulative fixes for a specific version of Sterling Integrator. Patch files are available on the Sterling Commerce Support on Demand web site. Because each patch contains the fixes from previous patches, you only need to install the most recent patch.

Note: During patch installation, the dbVerify utility compares the list of standard indexes with those present in the database and drops the custom indexes. You should recreate the custom indexes after the patch installation is complete.

Patch files are named using the following naming convention:

si_<release number>_build_<build number>.jar

Information about a patch is located in a PDF file with a similar name. The naming convention for PDF files containing information about a particular patch is:

si_<release number>_build_<build number>_patch_info.pdf

Before you install the patch, review the following items:

- Preserve your custom changes to system resources.
- The patch installation may use one or more patch property override files. These files will be named *propertyFile_patch.properties*. Do not alter these files.
- Property changes made directly in *.properties or *.properties.in files may be overwritten during the patch installation. Properties overridden using the customer_overrides.properties file are not affected. Sterling Commerce recommends that you maintain property file changes using (when possible) the customer_overrides.properties file. For more information about this file, refer to the property file documentation.
- If you edited any of the cdinterop files, you must back them up before applying the patch. The cdinterop files do not have initialization (*.in) files. After applying the patch, use the backup version of the files in your patched installation. These files include the following files: cdinterop-proxy-records.properties; cdinterop-spoe-auth.properties; cdinterop-spoe-policy.properties; and cdinterop-user-records.properties.
- Information about the patch installation is automatically logged to *\install_dir\install\logs\InstallService.log*.
- If you need to rollback a patch, see the *Patch Change Report*.

Preserve Custom Changes in Windows Cluster Environment

About this task

As part of a default cluster configuration, certain values in the database for service or adapter configurations, and default document storage, need to be updated to get the cluster working. The default settings do not include a shared or mounted file system with a line of sight from all cluster nodes. Certain service or adapter configurations are forcibly deployed on node 1 and the default document storage type is set up to "Database" for all business processes.

To keep these custom configuration changes from being overwritten, you can run the following cluster configuration script:

```
startCluster.cmd nodeNumber true/false
```

Where:

- nodeNumber is the cluster node number
- True performs database updates
- False prevents data base updates.

The first time you configure a cluster, you need to have the option set to true. After the first configuration, you can use the false option. The false option prevents any configuration changes from affecting the system, especially after installation a patch or hot fix.

Install a Critical Maintenance Patch to the Cluster (Windows)

About this task

To install a critical patch to the entire cluster in a Windows environment (where you need to stop the entire cluster):

Procedure

1. Go to the Sterling Commerce Support on Demand Web site, at <https://support.sterlingcommerce.com/user/login.aspx>.
2. Download the most recent patch file for your version of Sterling Integrator and record the absolute path to the downloaded file. Do not rename the file. If you use FTP, you must use Binary mode.
3. Verify that the database server is up and ready to accept connections.
4. Stop all the nodes in the cluster.
5. Perform a full backup of the Sterling Integrator installation directory, including all subdirectories.
6. Perform a backup of the database.
7. If you edited any property files, ensure that the associated properties.in files have the most current changes. Property files will be overwritten with the contents of the associated properties.in files during the patch installation.
8. Is the database password encrypted? If Yes, decrypt the password.
9. Close all command prompt windows.
10. Navigate to `install_dir` for the node (starting with node 1), using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none">• Click Start.• Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

11. Enter: `InstallService.cmd <path>\si_<version>_sp_0_patch_<number>_<app_server>.jar`
where:

`<path>` is fully qualified path to maintenance patch file
`<version>` is Sterling Integrator version
`<number>` is patch number
`<app_server>` is Application server

If the patch attempts to modify the database schema and the modification fails, you will receive an error message about the failure. The message will provide the error message code from the database and the SQL command that failed. The failure information is also logged to the system.log file (in the `\install_dir\install` directory) and to the patch.log file.

12. Press **Enter** to continue.
13. If you want to accept the license agreement, enter `Y`.
14. Enter the passphrase.

Information about the patch is displayed. After the patch has been applied, the following message is displayed: Deployment to application server successful.

15. After you have completed the patch for node 1, you can now perform the steps for node 2 and greater. For node 2 and greater, you must update the value of REINTDB to false. When REINTDB is false, database updates are not applied during each patch. The REINTDB attribute is in the `\install_dir\install\properties\sandbox.cfg` file.
16. Repeat Steps 10 to 14 to apply the patch to each node.
17. If you decrypted the database password, re-encrypt the password.
18. For each node, navigate to the `install_dir` and start the nodes, using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
<ul style="list-style-type: none"> • Open a command prompt window (from the Run dialog box). • Enter <code>startCluster.cmd nodeNumber</code>. 	<p>Complete the following steps:</p> <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. <p>The Administrator: Command Prompt dialog box is displayed.</p> <ul style="list-style-type: none"> • Enter <code>startCluster.cmd nodeNumber</code>.

19. Restart Sterling Integrator.
If you are using a perimeter server in the DMZ, you will to review the information on apply a patch to the perimeter server.

Install a Maintenance Patch One Node at Time to the Cluster (Windows)

About this task

To install a patch to the one node at a time in a Windows Cluster environment, starting with node 1:

Procedure

1. Go to the Sterling Commerce Support on Demand Web site, at <https://support.sterlingcommerce.com/user/login.aspx>.
2. Download the most recent patch file for your version of Sterling Integrator and record the absolute path to the downloaded file. Do not rename the file. If you use FTP, you must use Binary mode.
3. Verify that the database server is up and ready to accept connections.
4. Navigate to `\install_dir\install\bin` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	<p>Complete the following steps:</p> <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. <p>The Administrator: Command Prompt dialog box is displayed.</p>

5. Enter `hardstop.cmd` to stop the node. Wait until the perimeter server of the node is completely down before installing the patch.
6. Perform a full backup of the Sterling Integrator installation directory, including all subdirectories.
7. Perform a back up of the database.
8. If you edited any property files, ensure that the associated `properties.in` files have the most current changes. Property files will be overwritten with the contents of the associated `properties.in` files during the patch installation.
9. Is the database password encrypted? If Yes, decrypt the password.
10. Close all command prompt windows.
11. Navigate to installation directory, using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. <p>The Administrator: Command Prompt dialog box is displayed.</p>

12. Enter: `InstallService.cmd <path>\si_<version>_sp_0_patch_<number>_<app_server>.jar`

where:

`<path>` is fully qualified path to maintenance patch file

`<version>` is Sterling Integrator version

`<number>` is patch number

`<app_server>` is Application server

If the patch attempts to modify the database schema and the modification fails, you will receive an error message about the failure. The message will provide the error message code from the database and the SQL command that failed. The failure information is also logged to the `system.log` file (in the `install_dir\install` directory) and to the `patch.log` file.

13. Press **Enter** to continue.
14. If you want to accept the license agreement, enter `Y`.
15. Enter the passphrase.
Information about the patch is displayed. After the patch has been applied, the following message is displayed: Deployment to application server successful
16. After you have completed the patch for node 1, you can now perform the steps for node 2 and greater. For node 2 and greater, you must update the value of `REINTDB` to false. When `REINTDB` is false, database updates are not applied during each patch. The `REINTDB` attribute is in the `install_dir\install\properties\sandbox.cfg` file.
17. Repeat Steps 11 to 15 for each node.
18. If you decrypted the database password, re-encrypt the password.
19. Start Sterling Integrator.
If you are using a perimeter server in the DMZ, you will to review the information on apply a patch to the perimeter server.

Install a Hot-Fix (Windows Cluster)

About this task

After you install the Sterling Integrator you may need to install a hot-fix. A hot-fix is one or more fixes applied to a specific existing patch.

Before you can install a hot-fix developed for your company, you must have completed the following:

- Received the file name of the `ccaseid.jar` to install from Sterling Commerce Customer Support
- Created a full backup of the Sterling Integrator
- Created a full backup of your database
- Preserve your custom changes to system resources.

To install a hot-fix in a Windows Cluster environment, starting with node 1:

Procedure

1. Log in to the computer that you are installing the hot-fix on.
2. If the database password was encrypted, decrypt the password.
3. Enter `ftp theworld.stercomm.com`.
4. Enter your user name and password. If you do not know your user name and password, contact Sterling Commerce Customer Support.
5. Enter `bin` and press **Enter** to select Binary as your transfer mode.
6. At the FTP prompt, enter `get ccaseid.jar`, where `ccaseid` includes the ID number you received from Customer Support.
7. Stop the Sterling Integrator.
8. Navigate to `install_dir` for the node (starting with node 1), using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none">• Click Start.• Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

9. Enter `installService.cmd \absolutePath\ccaseid.jar` to install the hot-fix. You may need to complete this step twice depending on the patch. Read the output from the `InstallService` script carefully to see if you need to complete this step twice.
10. After you have completed the hot-fix for node 1, you can now perform the steps for node 2 and greater. For node 2 and greater, you must update the value of `REINTDB` to false. When `REINTDB` is false, database updates are not applied during each patch. The `REINTDB` attribute is in the `\install_dir\install\properties\sandbox.cfg` file.
11. Repeat Steps 8 and 9 for each node.
12. If you decrypted the database password, re-encrypt the password.
13. For each node, navigate to the `install_dir` (starting with node 1) and start the cluster, using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
<ul style="list-style-type: none"> • Open a command prompt window (from the Run dialog box). • Enter <code>startCluster.cmd nodeNumber</code> 	Complete the following steps: <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed. • Enter <code>startCluster.cmd nodeNumber</code>

14. Start the Sterling Integrator.
15. Navigate to the `install_dir\install\bin` directory, run the `dump_info` command to verify that the hot-fix was successfully installed, using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
<ul style="list-style-type: none"> • Open a command prompt window (from the Run dialog box). • Enter <code>dump_info.cmd</code> 	Complete the following steps: <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed. • Enter <code>dump_info.cmd</code>

Uninstalling an interim fix

Uninstalling an interim fix is a manual process. IBM support must first determine what is included in the interim fix you want to remove, and then manually backout the changes one at a time. The complexity of this process, therefore, can vary greatly.

If you must remove an interim fix, contact IBM support by creating a PMR (Problem Management Record)

DB Checksum Tool

A checksum is a simple redundancy check used to detect errors in data. In Sterling Integrator 5.1, a verification process is used to compare the checksum between the existing default resource and the resource added after applying a patch or upgrading. The DB Checksum tool, a resource difference tool generates a granular report of the changes in the system that was not permitted to be set as defaults.

The DB Checksum tool generates the difference in resource checksum between the default resource and the latest system resource from the database.

Perform a Checksum (Windows)

About this task

To run the DB Checksum tool in the Windows environment:

Procedure

1. Navigate to `\install_dir\bin` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none">• Click Start.• Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

2. Enter `db_checksum_tool.cmd [-d] [-i [1 | 2 | 3 | 4 | 5]] [-r [wfd | map | schema | sii | template]] [-o <output file>] [-g]`

Where:

-d is the mode to dump the difference of resource checksum between the default resource and latest system resource.

-i is the resource type integer (optional).

1 is WFD.

2 is MAP.

3 is SCHEMA.

4 is SII.

5 is TEMPLATE.

-r is the resource name (optional). For example, wfd, map, schema, sii, or template.

-o is the file name to output all the messages (optional).

-g is the file name that lists all the ignored resources (optional).

-h is the help screen.

The DB Checksum tool performs the relevant checksum operation based on the command options and generates the output message.

Patch Changes Report

The Patch Changes Report is used to obtain information if you need to rollback a patch. The patch report can be found in the installation directory `patch_reports` folder. The report contains the following patch information:

- Patch ID
- Patch Changes
- Number of files deleted
- Number of JARs removed
- Number of JARs added
- Number of files added
- Number of files changed
- Number of properties added
- Number of business processes added
- Number of service instances added
- Number of service definitions added
- Number of templates added
- Number of reports added

- Number of maps added
- Number of schemas added
- Number of business rules added

For example, the installation directory patch_reports folder contains the file Patch_Report.html. When you open this html file, you can view the patch information.

Example: Patch Changes Report

The following is an example of a Patch Changes Report.

Summary of Changes

Patch ID: Platform_2.0
 Patch Changes: 1287
 Number of Files Deleted: 0
 Number of JARs Removed: 2
 Number of JARs Added: 0
 Number of Files Added: 3
 Number of Files Changed: 3
 Number of Properties Added: 4
 Number of BPs Added: 4
 Number of Service Instances Added: 2
 Number of Service Definitions Added: 3
 Number of Templates Added: 0
 Number of Reports Added: 0
 Number of Maps Added: 3
 Number of Schemas Added: 3
 Number of Business Rules Added: 0

List of JARs Removed:

JAR Removed: /SAMPLE_INSTALL_1/jar/jaf/1_0_2/activation.jar
 Time: Wed May 13 15:23:08 EDT 2009
 JAR Removed: /SAMPLE_INSTALL_1/jar/commons_logging/1_0_3/commons-logging-api.jar
 Time: Wed May 13 15:23:08 EDT 2009

List of Files Added:

File Added: /SAMPLE_INSTALL_1/bin/sql/fix_db2_schema.sql
 Time: Wed May 13 15:21:30 EDT 2009
 File Added: /SAMPLE_INSTALL_1/bin/sql/fix_db2iseries_schema.sql
 Time: Wed May 13 15:21:30 EDT 2009
 File Added: /SAMPLE_INSTALL_1/bin/errorQueueManager.sh.in
 Time: Wed May 13 15:21:30 EDT 2009

List of Files Changed:

File Changed: /SAMPLE_INSTALL_1/properties/lang/en/Reports_en.properties
 File Changed: /SAMPLE_INSTALL_1/properties/lang/es/Reports_es.properties
 File Changed: /SAMPLE_INSTALL_1/properties/lang/fr/Reports_fr.properties

List of Properties Added:

Property Added: /SAMPLE_INSTALL_1/properties/filesToRemove.txt
 Property Added: /SAMPLE_INSTALL_1/properties/filesToRemove.txt.in
 Property Added: /SAMPLE_INSTALL_1/properties/csr.properties.sample
 Property Added: /SAMPLE_INSTALL_1/properties/csr.properties.sample.in

List of BPs Added:

BP Added: Schedule_AssociateBPsToDocs.bpm1 version: 4
 Time: Wed May 13 15:23:07 EDT 2009
 BP Added: Recovery.bpm1 version: 17
 Time: Wed May 13 15:23:07 EDT 2009
 BP Added: Schedule_AutoTerminateService.bpm1 version: 10
 Time: Wed May 13 15:23:07 EDT 2009
 BP Added: Schedule_DBMonitorService.bpm1 version: 1
 Time: Wed May 13 15:23:08 EDT 2009

List of Service Instances Added:
Service Instance Added: RetentionProcessor version: 2
Time: Wed May 13 15:23:28 EDT 2009
Service Instance Added: MESAHttpServerAdapter version: 1
Time: Wed May 13 15:25:11 EDT 2009

List of Service Definitions Added:
Service Definition Added: LockServiceType
Time: Wed May 13 15:22:58 EDT 2009
Service Definition Added: XAPIServiceType
Time: Wed May 13 15:22:59 EDT 2009
Service Definition Added: CleanLockServiceType
Time: Wed May 13 15:22:59 EDT 2009

List of Templates Added:
Template Added: Normalize
Time: Wed May 13 15:23:26 EDT 2009
Template Added: Derive
Time: Wed May 13 15:23:26 EDT 2009

List of Maps Added:
Map Added: IBMPutResponseToXML
Time: Wed May 13 15:24:05 EDT 2009
Map Added: http_headers
Time: Wed May 13 15:24:36 EDT 2009
Map Added: OracleHttpHeaders
Time: Wed May 13 15:24:51 EDT 2009

List of Schemas Added:
Schema Added: E5_V20_Acknowledge_Result.dtd from file: E5_V20_Acknowledge_Result
Time: Wed May 13 15:24:36 EDT 2009
Schema Added: E5_V20_Acknowledge_Submit.dtd from file: E5_V20_Acknowledge_Submit
Time: Wed May 13 15:24:36 EDT 2009
Schema Added: E5_V20_APIs_Result.dtd from file: E5_V20_APIs_Result
Time: Wed May 13 15:24:36 EDT 2009

Chapter 8. Configure Non-English Environment in Windows

Non-English Environment Checklist

You can install the Sterling Integrator in an English or a non-English environment. The base language for the Configurator can be switched only once. Use the following checklist change to a non-english environment:

#	Non-English Environment Checklist	Your Notes
1	Install the Sterling Integrator Language Pack.	
2	Load the Sterling Integrator Language Pack Factory Defaults.	
3	Load the Sterling Integrator Language Pack translators.	
4	Configure Encodings.	
5	Configure Locales.	

Language Settings in a Windows Environment

Language settings for Java applications involve both character sets and encoding:

- A character set is a set of characters (letters, numbers, and symbols such as #, \$, and &) that are recognized by computer hardware and software.
- An encoding is a representation of data in a particular character set. An encoding set is a group of encodings.

For information about basic and extended encoding sets, see java.sun.com/j2se/1.5.0/docs/guide/intl/encoding.doc.html.

The default encoding set includes:

- UTF-8 (default)
- ISO-8859-1
- ISO-8859-5
- US-ASCII
- ISO_8859-1
- EUC-JP
- UTF-16
- ISO-2022-JP

The Sterling Integrator provides two property files that contain supported encoding sets. These properties files reside in the `\install_dir\install\properties` directory.

- `encodings.properties` – Contains the default encoding set used in the user interface.
- `encodings_large.properties` – Contains all supported encoding sets.

You are not limited to the encodings in the `encoding.properties` file. The Sterling Integrator enables you to configure the `encodings.properties` files to expand the number of encodings you can use.

Install the Language Pack (Windows)

About this task

Before installing the language pack be sure that you have successfully installed Sterling Integrator.

To install Sterling Integrator language pack:

Procedure

1. Insert the language CDs into your CD-ROM drive.
2. Navigate to Win Directory using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none">• Click Start.• Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

3. Run the `setup.exe` command.

Load the Language Pack Translations (Windows)

About this task

Prior to loading the Sterling Integrator Language Pack factory defaults, be sure that you have successfully completed all instructions in the database chapter.

To load the language pack translation with custom localization literals:

Procedure

1. Navigate to `\install_dir\install\bin` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none">• Click Start.• Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

2. Run the LocalizedStringReconciler tool in the IMPORT mode, enter: `ant.cmd -f localizedstringreconciler.xml import -Dsrc=install_dir\database\FactorySetup\XMLS`

This tool first inserts the value specified in the `<from_language>_<from_country>_ycplocalizedstrings_<to_language>_<to_country>` > .properties file present in the `install_dir\database\FactorySetup\XMLS\<language>_<country>` directory into the database.

The basefilename refers to the file present in the `\database\FactorySetup\XMLS` directory, for which the translations are to be imported into the database.

3. Verify that your locale settings such as currency, time format, and date are correct.

Configure Encodings for the Sterling Integrator (Windows)

About this task

To configure your encoding set:

Procedure

1. Stop the Sterling Integrator and wait for shutdown to complete.
2. Navigate to `\install_dir\install\bin` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

3. Open the `encodings_large.properties` file.
4. Select the encodings you want to add to the `encodings.properties` file.
5. Open the `encodings.properties.in` file.
6. At the end of the `encodings.properties.in` file, add the encodings you selected from the `encodings_large.properties` file. When adding encodings from one file to the other, first copy the encodings as they appear in the `encodings_large.properties` file. After adding the new encodings, ensure that the index numbers are consecutive. If the index numbers are not consecutive, change the index number or numbers as needed. For example, `encoding54` cannot follow `encoding6`. In this example, change `encoding54` to `encoding7`.
The first name in the definition (before the comma) is the name that will appear in the Sterling Integrator user interface. You can change this name to make it more descriptive. For example: `encoding4 = 819,ISO8859_1` may be changed to `encoding4 = WesternEurope,ISO8859_1`. `ISO8859_1` is the Java canonical name and should not be changed.
7. Update the first line in the `encodings.properties.in` file (`numberof`). Change *numberof* to the number of encodings added to the file. For example, if the current value is `numberof = 6` and you add 5 new encodings, the new value is `numberof = 11`.
numberof indicates the total number of encodings located in the file. You must update `numberof` to ensure that the encodings you added will be visible in the user interface.
8. Navigate to `\install_dir\install\bin` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

9. Enter `setupfiles.cmd`.
10. Start Sterling Integrator.

Configure Locales (Windows)

About this task

The Sterling Integrator runs in any locale that Java supports. If you want to run in a non-default locale, then configure your environment to the specific locale you want to use.

To determine and set your locale in a windows environment:

Procedure

1. Select **Control Panel > Regional Options > General**.
2. From the Your locale (location) list, select the language and location.
3. Click **Set Default** and select the locale from the Set the appropriate locale list.
4. To configure your operating system as a non-English environment, consult your operating system's documentation.

Load the Language Pack Factory Defaults (Windows)

About this task

To load the language-specific factory defaults, use the `loadDefaults.cmd` script available in the `install_dir\install\bin` directory and pass the locale-specific installer file.

For example:

```
loadDefaults.cmd \install_dir\install\database\FactorySetup\install\  
<language>_<country>_locale_installer.xml
```

The default locale that is shipped with the CD is `ja_JP`.

Chapter 9. User Documentation

Sterling Integrator User Documentation

The user documentation is available via an online documentation site on the Web. Providing the documentation in an online environment allows for frequent updates of content based on user feedback and usability.

We also understand the need for a printed copy of documentation. You can print topics of information using your Internet browser, or you can download documents in PDF format. You also have the option to request a documentation CD.

Access the Online Documentation


About this task

You can also access the Documentation site by opening your Internet browser and entering the following URL:

<http://www.sterlingcommerce.com/Documentation/SI51/homepage.htm>

After you are in the documentation library, you can:

- Enter a word or phrase and search the entire library for information.
- Move through a hierarchy of contents pages to identify the topic you want to read or print.
- Print topics by using your browser's Print function.
- Download entire documents in PDF format. To download PDF documents, click the Documentation in PDF Format link from the main online documentation page.

To access the Documentation site from within Sterling Integrator or one of its tools, select the Help  icon. The application must reside on a computer that supports Internet access and an Internet browser.

Request a Documentation CD

About this task

You can request a CD that contains all the documentation found on the Documentation site. To submit a request, go to the following URL:

http://support.sterlingcommerce.com/forms/Gentran_GIS_UpgradeRequest.aspx

Chapter 10. Perimeter Server Installation

Perimeter Server Overview

A perimeter server is an optional software tool for communications management. A perimeter server can be installed in a demilitarized zone (DMZ). A DMZ is a computer host or small network inserted as a neutral zone between a company's private network and their public network. A perimeter server requires a corresponding perimeter client.

The perimeter server manages the communications flow between outer layers of your network and the TCP-based transport adapters. A perimeter server can solve problems with network congestion, security, and scalability, especially in high-volume, Internet-gateway environments.

Installation Guidelines for Perimeter Servers with Sterling Integrator

The installation program installs a perimeter client and a local mode server. The local mode server is useful for testing purposes or in environments that do not require a secure solution. However, if you require high-volume, secure connections, you must install a perimeter server in a remote zone, either a more secure or less secure network than your integration server.

Consider the following before you install a perimeter server:

- Licensing for a perimeter server is determined by the licensing restrictions on the corresponding B2B adapters.
- Each perimeter server is limited to two TCP/IP addresses:
 - Internal interface is the TCP/IP address that the perimeter server uses to communicate with the Sterling Integrator.
 - External interface is the TCP/IP address that the perimeter server uses to communicate with trading partners. To use additional TCP/IP addresses, install additional perimeter servers.
- You can have multiple perimeter servers installed on the same computer interacting with one instance of Sterling Integrator. To install a perimeter server on a computer with an existing instance, install the new perimeter server in a different installation directory.
- The combination of internal TCP/IP address and port must be unique for all perimeter servers installed on one computer.
 - If a perimeter server is installed using the wildcard address, then all ports must be unique. The assigned ports are not available for use by adapters that use the server or any other perimeter server on that computer.
 - The internal and external interface may use the same TCP/IP address. However, the port used by the perimeter server is not available to the adapters that use the server.

Perimeter Server Installation Methods

You can install perimeter server either in silent mode or in interactive mode. The default installation mode is silent. In the silent mode, you should specify the details in a silent file, whereas in the interactive mode, you should enter the value each time a prompt appears.

Perimeter Server Information Gathering Checklist

Before you install the perimeter server, you need to gather the following information and answer the following questions:

Perimeter Server Information Gathering Checklist	Your Notes
Path to java	
Path to the Sterling Integrator installation directory	
Will this perimeter server be installed in a less secure network?	
TCP/IP address or the DNS address that the perimeter server will listen on.	
Listening port for the perimeter server.	
Local port that the perimeter server will use to connect to Sterling Integrator.	
Port number must be higher than 1024.	

Perimeter Server Security Vulnerabilities

When the Sterling Integrator is deployed with a remote perimeter server in a more secure network zone, there is a security vulnerability. An intruder may compromise the host where the proxy resides, and take over the persistent connection to the perimeter server residing in the more secure zone. If this happens, the perimeter server will relay all the intruder's network requests past the firewall into this internal zone.

To prevent an intrusion, limit the activities the remote perimeter server can perform on behalf of the proxy to specifically those activities that the proxy needs to do for its operation.

Control these limitations by using a configuration residing in the secure network zone with the remote perimeter server, inaccessible by the proxy that could become compromised.

Install a Perimeter Server in a Less Secure Network (Windows)

About this task

To install a perimeter server in a Windows environment in interactive mode:

Procedure

1. Close all open Windows programs.
2. Copy the ps_4500.jar installation files from the installation media to a Windows directory. If you are using FTP to copy the file, make sure your session is set to binary mode.
3. To start the perimeter server installation, use one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
<ul style="list-style-type: none"> • From a command prompt (or from the Run dialog box), enter the following command: <pre data-bbox="488 323 850 411">\path_to_java\java -jar \install_dir\install\packages\ ps_4500.jar -interactive</pre> 	<ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed. • Enter the following command: <pre data-bbox="992 401 1354 512">path_to_java\java -jar install_dir\install\packages\ ps_4500.jar -interactive</pre>

The installation program verifies the operating system, required patch level, and the location and version of the JDK.

4. Enter the full path name of the installation directory.
5. If there is an existing installation in the directory you specify, you can update it using the same settings. Answer the question:
There is an existing install at that location, update it while keeping existing settings?
If **yes**, the installation will proceed without additional entries.

Note: If you want to change any of the settings, you must use a new directory, or delete the old installation before performing the new installation. You cannot overwrite an existing installation, and you cannot use an existing directory that does not contain a valid installation. The existing installation must be Sterling Integrator 5.1 or later.

6. Confirm that the installation directory is correct.
The program verifies the amount of available disk space.
7. Answer the question:
Is this server in a less secure network than the integration server?
Yes
8. Answer the question:
Will this server need to operate on specific network interfaces?
If **yes**, the program returns a list of the network interfaces available on your host. Select the interfaces for the server to use.
9. Enter the TCP/IP address or DNS name for the internal interface to use to communicate with the integration server (Sterling Integrator). Press **Enter** to use a wildcard for this address.
10. Verify the TCP/IP address or DNS name for the internal interface.
11. Enter the TCP/IP address or DNS name for the external interface to use to communicate with trading partners. Press **Enter** to use a wildcard for this address.
12. Verify the TCP/IP address or DNS name for the external interface.
13. Enter the port that the perimeter server will listen on for the connection from integration server (Sterling Integrator). The port number must be higher than 1024.
14. Verify the port.
When the perimeter server is installed, the following message is displayed:
Installation of Perimeter Service is finished
15. Change to the installation directory.
16. Enter startupPs.cmd to start the perimeter server.

Install a Perimeter Server in a More Secure Network (Windows)

About this task

Before you begin:

- Sterling Integrator 5.1 needs to be installed.
- You should have completed the Perimeter Server Information Gathering Checklist.

To install a perimeter server in a more secure network in a Windows environment using the interactive mode:

Procedure

1. Close all open Windows programs.
2. Copy the ps_4500.jar installation files from the installation media to a Windows directory. If you are using FTP to copy the file, be sure your session is set to binary mode.
3. To start the perimeter server installation, use one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
<ul style="list-style-type: none">• From a command prompt (or from the Run dialog box), enter the following command: <pre>\path_to_java\java -jar \install_dir\install\packages\ ps_4500.jar -interactive</pre>	<ul style="list-style-type: none">• Click Start.• Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.• Enter the following command: <pre>path_to_java\java -jar \install_dir\install\packages\ ps_4500.jar -interactive</pre>

The installation program verifies the operating system, required patch level, and the location and version of the JDK.

4. Enter the full path name for the Sterling Integrator 5.1 installation directory and press **Enter**.
If there is an existing installation in the directory you specify, you can update it using the same settings. Enter yes, and installation will proceed without additional entries.
5. Enter yes to confirm that the installation directory is correct.
The program verifies the amount of available disk space.
6. Is this server in a less secure network than the integration server, enter no.
This installation is for a more secure network.
7. Will this perimeter server need to operate on specific network interface:
 - Enter yes to select from a list network interfaces available.
 - Enter no.
8. Enter the TCP/IP address or DNS name that the integration server will listen on for the connection from this perimeter server.
9. Enter yes to confirm the TCP/IP address or DNS name.
10. Enter the port that the integration server will listen on for the connection from this server. The port number must be higher than 1024.
11. Enter the local port number that the perimeter server will use for the connection to the integration server.

The port number must be higher than 1024, except specify a port of zero if you want the operating system to select any unused port.

12. Enter yes to confirm the port number.

After the installation is complete, the following messages are displayed:

```
Installation of Perimeter Service is finished
```

```
To start this Perimeter Server change to the install directory and run the startup script.
```

```
You will also need to configure this server in your integration server (SI) UI.
```

Silent Installation Method for an External Perimeter Server

You can install an external perimeter server using a silent install file. The perimeter server can be installed on the same machine where you have installed the Sterling Integrator or on a separate machine. It is recommended to install the perimeter server on an separate machine.

To use the silent installation method, you first create the silent install file and then you use to complete the installation.

Create the Silent Installation File for an External Perimeter Server

About this task

Create a silent installation file with the following variables:

Entry	Description
INSTALL_DIR	(Required) The installation directory that stores perimeter server files and related directories. This directory must exist prior to running the silent install.
REVERSE_CONNECT	(Optional) Determines if the perimeter server is to be installed in a more secure network zone. Valid values: <ul style="list-style-type: none"> • Y - more secure network zone • N - less secure network zone
PS_PORT	(Required) Determines the perimeter server port to interact with the system.
PS_SECURE_IF	(Required) Determines the TCP/IP address or DNS name for the internal interface to communicate with the integration server (Sterling Integrator). You can use a wildcard (*) for this address.
PS_EXTERNAL_IF	(Required) Determines the TCP/IP address or DNS name for the external interface to communicate with the trading partners. You can use a wildcard (*) for this address.
REMOTE_ADDR	(Optional) Determines the remote perimeter server address. (Not required if REVERSE_CONNECT=N)
REMOTE_PORT	(Optional) Determines the remote perimeter server port. (Not required if REVERSE_CONNECT=N)
MAX_JVM_HEAP	(Required) Determines the maximum Java heap size allocated to the JVM.

Install an External Perimeter Server with a Silent Installation File (Windows)

About this task

Before you begin, you should have already created the silent install file.

To install the external perimeter server using a silent installation file:

Procedure

1. From the installation media, copy SI.jar to a Windows directory.
2. Set up your silent installation file and record the file location.
3. To start the perimeter server silent installation, use one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
<ul style="list-style-type: none">• From a command prompt (or from the Run dialog box), enter the following command: <pre>\path_to_java\java -Xmx512m -jar \install_dir\install\packages\ ps_4500.jar -f silent.txt</pre>	<ul style="list-style-type: none">• Click Start.• Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.• Enter the following command: <pre>path_to_java\java -Xmx512m -jar \install_dir\install\packages\ ps_4500.jar -f silent.txt</pre>

The installation program verifies the operating system, required patch level, and the location and version of the JDK.

The installation starts. You can follow the progress of the installation on screen.

When the installation is finished, the system displays the following message:

Installation has completed successfully.

Install Patches in a Remote Perimeter Server (Windows)

About this task

Remote perimeter servers are not automatically updated by a service pack or patch. You must reinstall the perimeter server using the new perimeter server installation file supplied with the service pack or patch.

To update a Remote Perimeter Server:

Procedure

1. Update your installation with the latest maintenance patch. Obtain the maintenance patch file from the Sterling Commerce Support on Demand web site, at <https://support.sterlingcommerce.com>. These patches have a name that identifies a build number. For example, si_43_build_4307.jar. For more information, refer to the maintenance patch documentation.
2. Locate your perimeter server patch file in the *install_dir*\install\packages directory of your installation. For maintenance patches, obtain the file from the Sterling Commerce Support on Demand Web site, at <https://support.sterlingcommerce.com>. These patch files have a name that identifies a version number. For example, ps_2006.jar.
3. Copy the file to a directory on the remote server.

4. Stop the perimeter server.
5. Use one of the following methods to install the patch:

For Windows Server 2003 or earlier	For Windows Server 2008
<ul style="list-style-type: none"> • From a command prompt (or from the Run dialog box), enter the following command: <code>\absolutePath\bin\java -jar filename.jar -interactive</code> <p>Where the <i>absolutePath</i> is the directory name where the Java version is installed.</p>	<ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed. • Enter the following command: <code>\absolutePath\bin\java -jar filename.jar -interactive</code> <p>Where the <i>absolutePath</i> is the directory name where the Java version is installed.</p>

The program verifies the operating system, required patch level, and the location and version of the JDK.

6. Enter the full path to the installation directory. If you do not want to change any settings for your perimeter server, specify the same directory where the remote perimeter server was originally installed.
7. Answer the question:
 There is an existing install at that location, update it while keeping existing settings?
 If **yes**, the installation will proceed without additional entries.

Note: If you want to change any of the settings, you must use a new directory, or delete the old installation before performing the new installation. You cannot overwrite an existing installation, and you cannot use an existing directory that does not contain a valid installation. The existing installation must be Sterling Integrator 5.1 or later.

When the perimeter server is installed, the following message is displayed:
 Installation of Perimeter Service is finished

8. Change to the installation directory.
9. Start the perimeter server.

Grant Permissions for Specific Activities for a Perimeter Server

About this task

Before you begin:

- Remote perimeter server must be installed for a more secure zone.
- Know what permissions you want to grant
- Understand the content of the restricted.policy file. The first two grant sections in the restricted.policy file are required for correct perimeter server operation. Do not modify these sections.

Procedure

1. Install a remote perimeter server, choosing the option for a more secure network zone.
2. At the installation prompt *Is this server in a less secure network than the integration server?*, select **No**, which is the option for a more secure network zone.

3. Navigate to the perimeter server installation directory.
4. Open the restricted.policy file.
5. Add permission lines for each back-end server that you intend to allow the proxy to access. There are commented out examples for each type of server. The first two grant sections are required for correct perimeter server operation. Do not modify these sections.

For example, you can grant permission to a target FTP Server. In the example, servers are configured to listen on the following ports: 33001 (for FTP), 33002 (for HTTP), and 1364 (for C:D). These port numbers can be edited.

```
// To restrict or permit the required Host/Server to communicate with the
PS, update the "ftphost/httpthost/snode" with that of the Server IP and
provide the appropriate PORT number where the Server will listen. //
// For each target FTP Server
// permission java.net.SocketPermission "10.117.15.87:33001", "connect"; //
Control connection.
// permission java.net.SocketPermission "10.117.15.87:lowPort-highPort",
"connect"; // Passive data connections.
// 10.117.15.87 indicates IP of the FTP Server for which the permission is
granted by PS for communicating with client //
// For each target HTTP Server
//
// permission java.net.SocketPermission "10.117.15.87:33002", "connect";
// 10.117.15.87 indicates IP of the HTTP Server for which the permission
is granted by PS for communicating with client //

// For each target C:D snode
//
// permission java.net.SocketPermission "snode:1364", "connect";
// 10.117.15.87 indicates IP of the Connect Direct Node for which
the permission is granted by PS for communication //
```

6. In the perimeter server installation directory, there is the perimeter server settings file called remote_perimeter.properties. Edit it to change the "restricted" setting to a value of true to turn on restrictions.
7. In the future, any attempt by the perimeter server to access disallowed network resources will be rejected and logged in the perimeter server log written to the perimeter server installation directory.

Perform DNS Lookup on Remote Perimeter Server

About this task

By default, a perimeter server performs DNS lookup in the main server JVM. If you have limited DNS in your secure area, you can configure the remote perimeter server to look up trading partner addresses in the DMZ.

To enable DNS lookup to occur at the remote perimeter server, edit the remote_perimeter.properties file and change the following parameter:

Property Name	Description
<psname>.forceRemoteDNS	Forces resolution of DNS names at remote PS. Value is true or false.

Start Perimeter Servers (Windows)

About this task

To start a perimeter server in Windows:

Procedure

1. Navigate to the perimeter server installation directory.
2. Navigate to perimeter server installation directory using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none">• Click Start.• Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

3. Enter startupPs.cmd.

Stop Perimeter Servers in (Windows)

About this task

To stop a perimeter server in Windows:

Procedure

1. Navigate to perimeter server installation directory using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none">• Click Start.• Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

2. Enter stopPs.cmd.

Chapter 11. Uninstall the Software

Uninstall the Sterling Integrator from a Windows Cluster Environment

About this task

When you uninstall the Sterling Integrator, the Sterling Integrator is automatically removed from the server.

Additionally, you may perform the following tasks:

- Manually remove the JDK that was installed
- Manually remove any desktop tools that were downloaded
- Free any database space in Oracle, Microsoft SQL Server, or DB2 databases

To uninstall the Sterling Integrator from a Windows environment, perform the following steps for each node:

Procedure

1. Navigate to `\install_dir\install\bin` using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none">• Click Start.• Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

2. Enter `hardstop.cmd`. Wait for the shutdown to complete. If you begin removing files before all business processes and the system is stopped, you may be unable to remove the Sterling Integrator successfully.
3. Back up the file system and database.
This step is optional. However, by backing up the file system and database, you are ensured that the Sterling Integrator is completely recoverable.
4. Remove the installation directory by entering the following command in the parent directory of your installation directory: `rm -rf install_dir`
5. If you use an Oracle, Microsoft SQL Server, or DB2 database, these remain intact even after you remove the Sterling Integrator from the server. If you no longer want to reference the data, contact your database administrator about removing unwanted tables and recovering the database space where the Sterling Integrator used to reside.
6. Navigate into the `_uninst` subdirectory of your JDK installation directory using one of the following methods:

For Windows Server 2003 or earlier	For Windows Server 2008
Open a command prompt window (from the Run dialog box).	Complete the following steps: <ul style="list-style-type: none"> • Click Start. • Right-click Command Prompt and select Run as administrator. The Administrator: Command Prompt dialog box is displayed.

7. To manually remove the JDK, enter `uninstall.cmd`.
8. After you remove the Sterling Integrator from the server, you can remove Eclipse, and any tools that were downloaded to the desktop, including the following:
 - Map Editor and associated standards
Refer to the *Map Editor Guide* for information about removing the Map Editor.
 - Graphical Process Modeler
Refer to the *Graphical Process Modeler Guide* for information about removing the Graphical Process Modeler.
 - Web Template Designer
Refer to the *Web Extensions Guide* for information about removing the Web Template Designer.
 - (If licensed) MESA Developer Studio plug-ins, including:
 - MESA Developer Studio Software Development Kit (SDK)
 - MESA Developer Studio Skin Editor
 Refer to the *MESA Developer Studio* guide for information about removing MESA Developer Studio.
 - (If licensed) Reporting Services, which requires MESA Developer Studio if you want to use the plug-ins to create fact models and custom reports. Refer to the *MESA Developer Studio* guide for information about removing Reporting Services.

Chapter 12. Troubleshooting Tips for Windows

Troubleshooting Tips for Windows Environment

Situation	Message or Symptom	Explanation/Resolution
Installing	You encounter errors or problems during installation.	Explanation The installation creates several log files that you can use to diagnose problems like the failure of an installation. Resolution Examine the log files generated during installation: <ul style="list-style-type: none">• ant.install.log (in the <i>install_dir</i> directory)• <i>install_dir</i>\PreInstallSI.log
Installing	When you entered an absolute path during installation, a message indicated that the command was not found.	Explanation You entered an incorrect path. Check the information entered. Resolution Enter the correct path.
Installing	The license file cannot be found.	Explanation <ul style="list-style-type: none">• You did not obtain the license file.• The license file is corrupt.• You downloaded the license file to a PC but have not moved it to the server. Resolution You need to obtain the license file. If the license file resides on a PC, save the license file to the server.

Situation	Message or Symptom	Explanation/Resolution
Installing a desktop tool or resource	<p>Cannot download any of the following:</p> <ul style="list-style-type: none"> • Map Editor and associated standards • Graphical Process Modeler • Web Template Designer • (If licensed) MESA Developer Studio plug-ins, including: <ul style="list-style-type: none"> – MESA Developer Studio Software Development Kit (SDK) – MESA Developer Studio Skin Editor • (If licensed) Reporting Services, which requires MESA Developer Studio if you want to use the plug-ins to create fact models and custom reports. 	<p>Explanation</p> <p>When you install the Sterling Integrator, system files are created that contain an internal IP address. If you install the Sterling Integrator behind a firewall, and your firewall is configured to accept an external IP address from a client computer, you may not be able to download the desktop tools and resources. The firewall will reject the internal IP address from a client residing outside of the firewall.</p> <p>Resolution</p> <p>Modify the system files that contain the invalid IP address. Follow these steps:</p> <ol style="list-style-type: none"> 1. Navigate to <code>\install_dir\install\bin</code>. 2. Stop the Sterling Integrator. 3. Enter the following command followed by the external IP address: <code>patchJNLP.cmd external_IP_address</code> 4. Restart the Sterling Integrator.
Cluster Installation	<p>Cluster is not working properly and your machine is running dual-stack - ipv4 and ipv6.</p>	<p>Explanation</p> <p>You can see the node went down from User Interface, but the node is running.</p> <p>Resolution</p> <ul style="list-style-type: none"> • Find the ipv6 address in the <code>/etc/hosts</code> file and update the <code>noapp.properties.in</code> file <code>admin_host.2 = <ipv6_address></code>. • Edit the <code>jgroups_cluster.properties.in</code> file and replace the <code>&HOST_NAME</code> with the ipv6 address string and change <code>mcast_addr=FFFF::239.255.166.17</code>. • Enter <code>setupfiles.cmd</code>.

Notices

This information was developed for products and services offered in the U.S.A.

IBM® may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

1623-14, Shimotsuruma, Yamato-shi

Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be

incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

J46A/G4

555 Bailey Avenue

San Jose, CA 95141-1003

U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© IBM 2011. Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2011.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com)[®] are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at <http://www.ibm.com/legal/copytrade.shtml>.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium and the Ultrium Logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Connect Control Center®, Connect:Direct®, Connect:Enterprise®, Gentran®, Gentran®:Basic®, Gentran:Control®, Gentran:Director®, Gentran:Plus®, Gentran:Realtime®, Gentran:Server®, Gentran:Viewpoint®, Sterling Commerce™, Sterling Information Broker®, and Sterling Integrator® are trademarks or registered trademarks of Sterling Commerce®, Inc., an IBM Company.

Other company, product, and service names may be trademarks or service marks of others.



Product Number:

Printed in USA